AD-A103 061 GOLD (ROBERT) ASSOCIATES LOS ANGELES CA F/G 12/1

STUDY OF MULTISTATE PN SEQUENCES.(U)

JUL 81 N00173-80-C-0480

UNCLASSIFIED NL

1 of 1

END

DATE FILMED

9 81

DTIC

LEVEL II

ADA103061

STUDY OF MULTISTATE PN SEQUENCES

PROGRESS REPORT - PHASE I

CONTRACT NO. N00173-80-C-0480 new

PREPARED FOR

NAVAL RESEARCH LABORATORIES
WASHINGTON, D. C.

6 JULY 1981

PREPARED BY

ROBERT GOLD ASSOCIATES
435 SOUTH LA CIENEGA BOULEVARD
LOS ANGELES, CALIFORNIA 90048

STUDY OF MULTISTATE PN SEQUENCES

PROGRESS REP[redacted]T. ~~PHASE I~~

CONTRACT NO. N00173-80-C-0480

PREPARED FOR

NAVAL RESEARCH LABORATORIES
WASHINGTON, D.C.

6 JUL[redacted]81

APPRC
DISTI

PREPARED BY
ROBERT GOLD ASSOCIATES
435 SOUTH LA CIENEGA BOULEVARD
LOS ANGELES, CALIFORNIA 90048

A

TABLE OF CONTENTS

INTRODUCTION

This document is the Summary Progress Report submitted by Robert Gold Associates in accordance with the CDRL of Contract No. N00173-80-C-0480 and describes the work accomplished over the reporting period of September 17, 1980 through July 1, 1981 on the Study of Multistate Pseudonoise Sequences.

Although mainly binary encoding sequences have been used to date as the encoding mechanism for spread spectrum systems, and their employment has resulted in striking improvements in performance and operational capabilities over conventional communication systems, it has been recognized that further substantial improvements in spread spectrum communication systems could be economically achieved through an increased knowledge and application of multistate (as distinguished from binary) sequences.

The present work has been successful in extending the fundamental concepts and results of the theory of binary sequences to the multistate case. Substantial progress and new results have been achieved in the following areas:

1. Generation of Maximal Linear Multistate Sequences
2. Implementation of Multistate Sequences with Binary Logic Elements
3. Special Properties of Multistate Sequences
4. Definition and Computation of the Autocorrelation Function of Multistate Sequences
5. Computation of the Power Spectral Density of Maximal Linear Multistate Sequences

In Section 1 the multistate encoded signal and its analytical representation is reviewed to ensure that the properties of the multistate sequences which have the greatest impact on the resultant signals were emphasized during the current study.

In Section 2 the concept of a linear multistate sequence is discussed. The multistate alphabet (finite fields over $GF(2^k)$) and the polynomial corresponding to a feedback shift register are described. A method for implementing multistate sequences with binary logic elements is presented in this section. This result assures the practical and economical application of multistate

sequences. The concept of a maximal multistate sequence is discussed, and a method for determining maximal multistate polynomials is given. A table of irreducible polynomials of degree 2 for the 8-state case is constructed and presented in Section 2.5.

The autocorrelation function of multistate sequences is defined in Section 3, and the autocorrelation function of maximal linear multistate sequences is determined. The result is essentially independent of the period of the sequence and depends only on the number of states of the sequence. It is found that the autocorrelation function of multistate sequences has regularly spaced, relatively high out-of-phase autocorrelation peaks. In Section 3.8 we describe how these out-of-phase correlation sidelobes of a multistate maximal linear sequence may be used as an aid to rapid synchronization of pseudonoise encoded systems.

The power spectral density of maximal linear multistate sequences is determined in Section 3.8 where a formula for the spectral lines is given in terms of the discrete Fourier transform of a sequence of $2^k - 1$ values, where 2^k is the number of states. This formula allows the easy computation of the spectrum of multistate encoded signals. The power spectral density of a maximal 8-state sequence of period 63 is computed and presented in this section.

1. DEFINITION OF MULTISTATE SIGNAL AND ITS CORRELATION FUNCTION

Although the current study is concerned with the properties of the digital multistate sequences, which are the basic encoding mechanism for spread spectrum signals, it is important to define the role of these multistate sequences in determining the properties of the resultant signals. This will ensure that the direction of the current work can give priority to the study of those properties of the multistate sequences which have the greatest impact on the resultant signals and their application to tactical communication systems. Accordingly, a review of the analytical representation of pseudonoise signals and their correlation function was undertaken and documented. The basic formulas are summarized in what follows.

A pseudonoise signal which has been encoded by a multistate pseudorandom sequence may be represented analytically as

$$s(t) = \sum_{k=-\infty}^{\infty} \cos\left(\omega t + \gamma\big(a(k)\big)\right) f_0(t-\Delta k)$$

$$= \frac{1}{2}\,\mathrm{Re}\left[e^{i\omega t}\sum_{k=-\infty}^{\infty} e^{i\gamma(a(k))} f_0(t-\Delta k)\right]$$

where ω = carrier frequence

a = multistate sequence

γ = real valued mapping of multistate sequence which determines how the multistate sequence will operate on the carrier

f_0 = squarewave function; $f_0(t) = 1;\quad 0 \leq t < \Delta$

$f_0(t) = 0;\quad$ otherwise

Δ = code chip width.

Example: Let a be the 4-state sequence with values $0, 1, \beta, \beta^2$.

Let γ be the mapping such that

$$\gamma: \quad 0 \to \frac{\pi}{4}$$

$$1 \to \frac{-\pi}{4}$$

$$\beta \to \frac{3\pi}{4}$$

$$\beta^2 \to \frac{-3\pi}{4}$$

The resultant phase modulated signal is illustrated in Figure 1.

Code a	0	β	1	β^2
$\gamma(a)$	$\frac{\pi}{4}$	$\frac{3\pi}{4}$	$\frac{-\pi}{4}$	$\frac{-3\pi}{4}$

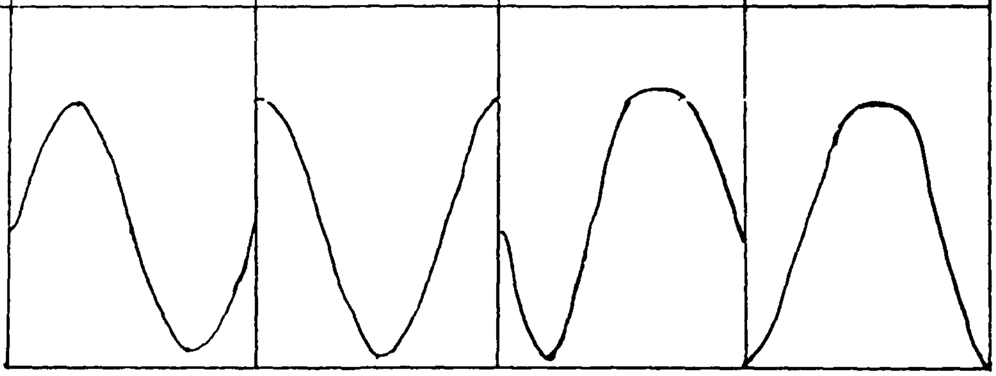


Figure 1. Four-phase modulated carrier

The correlation function of wideband PN signals is a crucial parameter in measuring their performance in spread spectrum systems. The cross-correlation function

$$R(s_a, s_b)(\tau) = \frac{1}{T} \int_0^T s_a(t) s_b(t-\tau)\, dt$$

of two pseudonoise signals $s_a(t)$ and $s_b(t)$ which have been encoded by two multistate sequences a and b, respectively, has been shown to be given by

$$R(s_a,s_b)(\tau) = \sum_{\ell=-\infty}^{\infty} \frac{1}{2} \mathrm{Re}\left\{e^{i\omega\tau} \frac{1}{p} \sum_{k=0}^{p-1} \eta\big(a(k)\big)\overline{\eta\big(b(k-\ell)\big)}\right\} R(f_0,f_0)(\tau-\Delta k)$$

where

$$\eta(a)(k) = e^{i\gamma(a(k))} \quad \text{and} \quad \eta(b) = e^{i\gamma(b(k))}.$$

In view of this result, the correlation function of two multistate sequences has been defined as follows [1, p. 97].

<u>Definition</u>: Let a and b be two multistate sequences of period p. Let η be any complex valued mapping of the sequence alphabet. The correlation function of the multistate sequence with respect to the mapping η is defined to be

$$\theta_\eta(a,b)(\tau) = \frac{1}{p} \sum_{k=0}^{p-1} \eta\big(a(k)\big)\overline{\eta\big(b(k-\tau)\big)}.$$

Thus,

$$R(s_a,s_b) = \sum_{\ell=-\infty}^{\infty} \frac{1}{2} \mathrm{Re}\{\theta^{i\omega\tau}\theta_\eta(a,b)(\ell)\} R(f_0,f_0)(\tau-\Delta\ell)$$

1.1 <u>Detection of Signal Encoded with Multistate Signal</u>

The received signal is given by

$$s_a(t) = \sum_{k=-\infty}^{\infty} \cos\Big(\omega_c t + \gamma(a(b))\Big) f_0(t-\Delta k)$$

$$= \frac{1}{2} \mathrm{Re}\left[e^{i\omega_c t} \sum_{k=-\infty}^{\infty} e^{i\gamma(a(k))} \cdot f_0(t-\Delta k)\right]$$

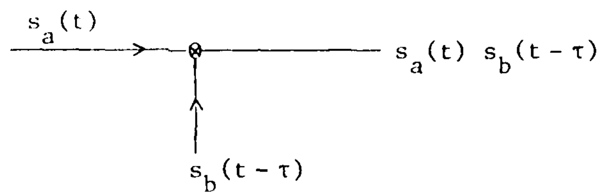
Let the locally generated signal be

$$s_b(t-\tau) = \sum_{k=-\infty}^{\infty} \cos\Big((\omega_c - \omega_1)t + \gamma(b(k))\Big)\; f_0(t - \tau - \Delta k)$$

where ω_1 is an IF frequency

$$= \frac{1}{2}\,\mathrm{Re}\left[e^{i(\omega_c - \omega_1)t} \sum_{k=-\infty}^{\infty} e^{i\gamma(b(k))}\; f_0(t - \tau - \Delta k)\right]$$

We first multiply the received signal $s_a(t)$ by the locally generated signal $s_b(t - \tau)$



Let

$$U_a(t) = \sum_{k=-\infty}^{\infty} e^{i\gamma(a(k))}\; f_0(t - \Delta k)$$

$$U_b(t) = \sum_{k=-\infty}^{\infty} e^{i\gamma(b(k))}\; f_0(t - \Delta k)$$

Then we have

$$s_a(t) = \frac{1}{2}\,\mathrm{Re}\left[e^{i\omega_c t}\; U_a(t)\right]$$

$$s_b(t) = \frac{1}{2}\,\mathrm{Re}\left[e^{i(\omega_c - \omega_1)t}\; U_b(t)\right]$$

$$s_a(t)s_b(t-\tau) = \frac{1}{4}\,\mathrm{Re}\left[e^{i\omega_c t}\; U_a(t)\right]\mathrm{Re}\left[e^{i(\omega_c - \omega_1)t}\; U_b(t-\tau)\right]$$

Using the relationship

$$\mathrm{Re}(z_1)\mathrm{Re}(z_2) = \frac{1}{2}\,\mathrm{Re}(z_1 \cdot z_2) + \frac{1}{2}\,\mathrm{Re}(\overline{z_1} \cdot z_2)$$

where z_1 and z_2 are complex numbers and bar indicates complex conjugation, we have

$$s_a(t)s_b(t-\tau) = \frac{1}{8}\,\mathrm{Re}\left[e^{i(2\omega_c - \omega_1)t}\,U_a(t)U_b(t-\tau)\right] + \frac{1}{8}\,\mathrm{Re}\left[e^{\omega_1 t}\,U_a(t)U_b(t-\tau)\right]$$

We now bandpass filter about the IF frequency ω_1 to obtain

$$y(t) = \frac{1}{8}\,\mathrm{Re}\left[e^{i\omega_1 t}\,U_a(t)U_b(t-\tau)\right]$$

and bandpass filter y(t) with a filter whose lowpass equivalent computes

$$\int_0^{\Delta P} U_a(t)U_b(t-\tau)\,dt$$

This integral has been shown to be equal to

$$\sum_{\ell=-\infty}^{\infty} \theta(a,b)(\ell)\;\theta(f_0,f_0)(\tau-\Delta\ell)$$

For $\tau = \ell k$, the above sum becomes $\theta(a,b)(k)$ and the output of the last bandpass filter is

$$z(t) = \frac{1}{8}\,\mathrm{Re}\left[e^{i\omega_1 t}\,\theta(a,b)(k)\right]$$

To envelope detect the waveform z(t) we square to obtain

$$z^2(t) = \frac{1}{128}\left\{\mathrm{Re}\left[e^{i2\omega_1 t}\,\theta^2(a,b)(k)\right] + \mathrm{Re}\left[\left|\theta(a,b)(k)\right|^2\right]\right\}$$

and lowpass filter to obtain $\dfrac{|\theta(a,b)(k)|^2}{128}$

2. MULTISTATE SHIFT REGISTER GENERATORS

2.1 The Multistate Alphabet

The set of symbols used for the multistate sequences which we shall initially consider are drawn from the Galois Field of 2^k elements, $GF(2^k)$. The addition and multiplication tables for these fields for k = 1, 2, and 3 are presented below.

Binary: $GF(2) = \{0,1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Four-state: $GF(4) = \{0,1,\beta,\beta^2\}$

+	0	1	β	β^2
0	0	1	β	β^2
1	1	0	β^2	β
β	β	β^2	0	1
β^2	β^2	β	1	0

·	0	1	β	β^2
0	0	0	0	0
1	0	1	β	β^2
β	0	β	β^2	1
β^2	0	β^2	1	β

Eight-state: $GF(8) = \{0,1,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6\}$

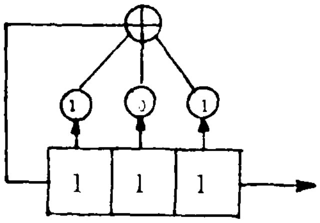
+	0	1	β	β^2	β^3	β^4	β^5	β^6
0	0	1	β	β^2	β^3	β^4	β^5	β^6
1	1	0	β^5	β^3	β^2	β^6	β	β^4
β	β	β^5	0	β^6	β^4	β^3	1	β^2
β^2	β^2	β^3	β^6	0	1	β^5	β^4	β
β^3	β^3	β^2	β^4	1	0	β	β^6	β^5
β^4	β^4	β^6	β^3	β^5	β	0	β^2	1
β^5	β^5	β	1	β^4	β^6	β^2	0	β^3
β^6	β^6	β^4	β^2	β	β^5	1	β^3	0

·	0	1	β	β^2	β^3	β^4	β^5	β^6
0	0	0	0	0	0	0	0	0
1	0	1	β	β^2	β^3	β^4	β^5	β^6
β	0	β	β^2	β^3	β^4	β^5	β^6	1
β^2	0	β^2	β^3	β^4	β^5	β^6	1	β
β^3	0	β^3	β^4	β^5	β^6	1	β	β^2
β^4	0	β^4	β^5	β^6	1	β	β^2	β^3
β^5	0	β^5	β^6	1	β	β^2	β^3	β^4
β^6	0	β^6	1	β	β^2	β^3	β^4	β^5

2.2 Multistate Feedback Shift Registers

Multistate sequences generated by feedback shift registers may be represented by polynomials with coefficients in the alphabet field of the sequence. Examples are given below for the binary, 4-state, and 8-state cases.

Binary



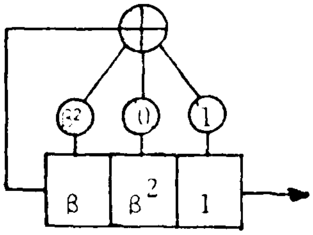
Output sequence a = 1 1 1 0 1

$$f(x) = 1 + 1x + 0x^2 + 1x^3$$

$$a = \frac{1}{f(x)} = \frac{1}{1 + 1x + 0x^2 + 1x^3}$$

$$= 1 + 1x + 1x^2 + 0x^3 + 1x^4 + \cdots$$

4-State



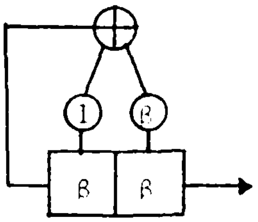
Output sequence a = 1 β^2 β 0 β^2

$$f(x) = 1 + \beta^2 x + 0x^2 + 1x^3$$

$$a = \frac{1}{f(x)} = \frac{1}{1 + \beta^2 x + x^3}$$

$$= 1 + \beta^2 x + \beta x^2 + 0x^3 + \beta^2 x^4 + \cdots$$

<u>8-State</u>



Output sequence $a = \beta\ \beta\ \beta^6\ \beta\ \beta^5$

$$\beta f(x) = 1 + 1x + \beta x^2$$

$$a = \frac{1}{f(x)} = \frac{\beta}{1 + x + \beta x^2}$$

$$= \beta + \beta x + \beta^6 x^2 + \beta x^3 + \cdots$$

The polynomial corresponding to a multistate shift register determines the properties of the multistate sequence generated by that shift register. Thus, to find the period of any polynomial f over $GF(2^n)$, multiply the polynomial by its conjugate polynomials to obtain a polynomial f' over GF(2). The period of f is equal to the period of f'.

<u>Example (4-state):</u> $GF(2^2)$ $f(x) = x^2 + \alpha x + 1$

The conjugate polynomial is $x^2 + \alpha^2 x + 1$

$$(x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1) = x^4 + x^3 + x^2 + x + 1 .$$

The period of $x^4 + x^3 + x^2 + x + 1$ is 5 and hence the period of $x^2 + \alpha x + 1$ (and $x^2 + \alpha^2 x + 1$) is 5, e.g.,

$$\frac{1}{x^2 + \alpha x + 1} = 1 + \alpha x + \alpha x^2 + x^3 + x^5 + \alpha x^6 + \cdots = 1\alpha\alpha 10|1\alpha\alpha 10| \cdots$$

<u>Example (8-state):</u> $GF(2^3)$ $f(x) = x^2 + \alpha^5 x + 1$

The conjugate polynomials are $(x^2 + \alpha^3 x + 1)$ and $(x^2 + \alpha^6 x + 1)$.

$$(x^2 + \alpha^5 x + 1)(x^2 + \alpha^3 x + 1)(x^2 + \alpha^6 x + 1) = x^6 + x^3 + 1 .$$

The period of $x^6 + x^3 + 1$ is 9 and hence the period of $f(x) = x^2 + \alpha^5 x + 1$ (and its conjugates) is also 9, e.g.,

$$\frac{1}{x^2 + \alpha^5 x + 1} = 1 + \alpha^5 x^2 + \alpha^2 x^2 + \alpha x^3 + \alpha x^4 + \alpha^2 x^5 + \alpha^5 x^6 + x^7 + x^9 + \alpha^5 x^{10}$$

$$= \underbrace{|1\ \alpha^5\ \alpha^2\ \alpha\ \alpha\ \alpha^2\ \alpha^5\ 1\ 0|}_{\text{period } 9}\ 1\ \alpha^5 \cdots$$

2.3 Polynomials Corresponding to Multistate Shift Registers

For the case of linear binary sequences, extensive tables of irreducible polynomials have been compiled [2] which determine the feedback taps for the shift registers which generate the sequences. The properties of the sequences generated by the shift registers may be determined from the algebraic properties of the corresponding polynomial. A method of determining the polynomials for multistate sequences having prescribed properties has been developed and is described in this section. The method assumes that tables of polynomials for the binary case are available.

Result: To find a polynomial $f(x)$ of degree k corresponding to a k-stage shift register which will generate a 2^m-state sequence of period p, we proceed as follows:

(1) Assume α is a root of a maximal binary polynomial $g(x)$ of degree $k \cdot m$.

(2) Choose an integer j such that

$$p = \frac{2^{m \cdot k} - 1}{\gcd(j, 2^{m \cdot k} - 1)}$$

(3) $f(x) = \prod_{i=0}^{k-1} (x + \alpha^{j \cdot 2^{i \cdot m}})$.

Example (4-state): $m = 2$

We construct a polynomial of degree 2 corresponding to a 2-stage shift register which will generate a $2^2 = 4$ state sequence of period $p = 5$.

(1) Let α be a root of the maximal binary polynomial of degree $m \cdot k = 4$ given by $g(x) = x^4 + x + 1$, i.e., $\alpha^4 = \alpha + 1$.

(2) Choose $j = 3$ such that

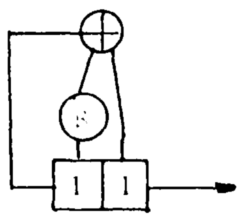
$$\frac{2^{m \cdot k} - 1}{\gcd(j, 2^{m \cdot k} - 1)} = \frac{2^4 - 1}{\gcd(3, 2^4 - 1)} = 5 .$$

(3) $f(x) = (x + \alpha^3)(x + \alpha^{12}) = x^2 + (\alpha^3 + \alpha^{12})x + 1$

$= x^2 + (\alpha^2 + \alpha + 1)x + 1 = x^2 + \alpha^{10}x + 1$

$f(x) = x^2 + \beta^2 x + 1$, where $\beta = \alpha^5$.

The shift register corresponding to this polynomial is



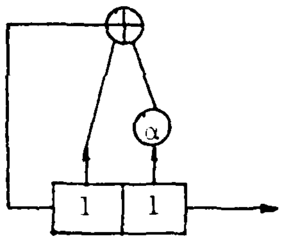
The sequences generated by this shift register have period 5, e.g.,

$$|1\ 1\ \beta\ 0\ \beta\ |1\ 1\ \cdots$$
$$|\text{ period } 5\ |$$

2.4 Implementation of Multistate Sequences

In this section, we explain how multistate sequences may be implemented with binary sequences generators. We shall use an 8-state sequence generator to illustrate the general procedure. We consider the maximal polynomial

over GF(8) given by $f(x) = \alpha x^2 + x + 1$. The shift register corresponding to this polynomial is



and the sequence $1/(\alpha^2 x^2 + x + 1)$ which is generated by this shift register with the indicated initial conditions is given by

$$\frac{1}{\alpha x^2 + x + 1} = 1 \;\; 1 \;\; \alpha^5 \;\; 1 \;\; \cdots$$

The complete sequence and its binary representation is shown in Figure 2.

In order to find the representation for the 8-state sequence as three binary sequences, we proceed with the following steps.

Step 1: Rationalize the polynomial representation of the 8-state sequence, e.g.,

$$\frac{1}{\alpha x^2 + x + 1} = \frac{1}{\alpha x^2 + x + 1} \quad \frac{(\alpha^2 x^2 + x + 1)(\alpha^4 x^2 + x + 1)}{(\alpha^2 x^2 + x + 1)(\alpha^4 x^2 + x + 1)}$$

$$= \frac{\alpha^6 x^4 + \alpha^5 x^3 + \alpha x^2 + 1}{x^6 + x^4 + x^3 + x + 1}$$

The denominator of the rationalized fraction provides the feedback taps for the required binary shift register.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	1	α^5	1	α^4	α^3	α^6	1	0	α	α	α^6	α	α^5	α^4	1	α	0	α^2	α^2	1	α^2	α^6	α^5	α	α^2	0	α^3	α^3	α	α^3	1	α^6	α^2	α^3
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	0	1	2	3	4	5	6
0	α^4	α^4	α^2	α^4	α	1	α^3	α^4	0	α^4	α^4	α^3	α^5	α^2	α	α^4	α^5	0	α^6	α^6	α^4	α^6	α^3	α^2	α^5	α^6	0	1	1	α^5	1	α^4	α^3	α^6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	1	1	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	0	0	0	1	1	0	1	1	0	0	1
0	0	1	0	1	0	1	0	0	1	1	1	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	0	0
0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	0	0	0	1	1	0	1	1	0	0	1	0	1	1	0	1	0	1	1	1
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	0	1	2	3	4	5	6
0	1	1	0	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	0	0	1	0	1	0	1	0	0	1	1	1	1	1	1	0
0	1	1	0	1	1	0	0	1	0	1	1	0	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	0	0	1	0	1	0	1
0	1	1	1	1	0	0	1	1	0	0	0	1	0	1	0	1	0	0	1	1	1	1	1	1	0	1	0	0	0	0	0	1	1	1

$0 \leftrightarrow 0\ 0\ 0$
$1 \leftrightarrow 1\ 0\ 0$
$\alpha \leftrightarrow 0\ 1\ 0$
$\alpha^2 \leftrightarrow 0\ 0\ 1$
$\alpha^3 \leftrightarrow 1\ 0\ 1$
$\alpha^4 \leftrightarrow 1\ 1\ 1$
$\alpha^5 \leftrightarrow 1\ 1\ 0$
$\alpha^6 \leftrightarrow 0\ 1\ 1$

Figure 2. Maximal 8-State Sequence and Its Binary Representation

<u>Step 2</u>: Express the coefficients of the numerator from GF(8) as binary triples, e.g.,

$$\alpha^6 = [0\ 1\ 1] \qquad \alpha = [0\ 1\ 0]$$

$$\alpha^5 = [1\ 1\ 0] \qquad 1 = [1\ 0\ 0]$$

$$\frac{\alpha^6 x^4 + \alpha^5 x^3 + \alpha x^2 + 1}{x^6 + x^4 + x^3 + x + 1} = \frac{[011]x^4 + [110]x^3 + [010]x^2 + [100]}{x^6 + x^4 + x^3 + x + 1}$$

<u>Step 3</u>: Write the fractional representation of the sequence given in Step 2 as the sum of three binary fractions, e.g.,

$$\frac{[011]x^4 + [110]x^3 + [010]x^2 + [100]}{x^6 + x^4 + x^3 + x + 1} =$$

$$\frac{x^3 + 1}{x^6 + x^4 + x^3 + x + 1} = 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad \cdots$$

$$\frac{x^4 + x^3 + x^2}{x^6 + x^4 + x^3 + x + 1} = 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad \cdots$$

$$\frac{x^4}{x^6 + x^4 + x^3 + x + 1} = 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad \cdots$$

$$1 \quad 1 \quad \alpha^5 \quad 1 \quad \alpha^4 \quad \alpha^3 \quad \alpha^6 \quad 1 \quad \cdots$$

The implementation of this 8-state sequence generator using a simple binary shift register is illustrated in Figure 3.

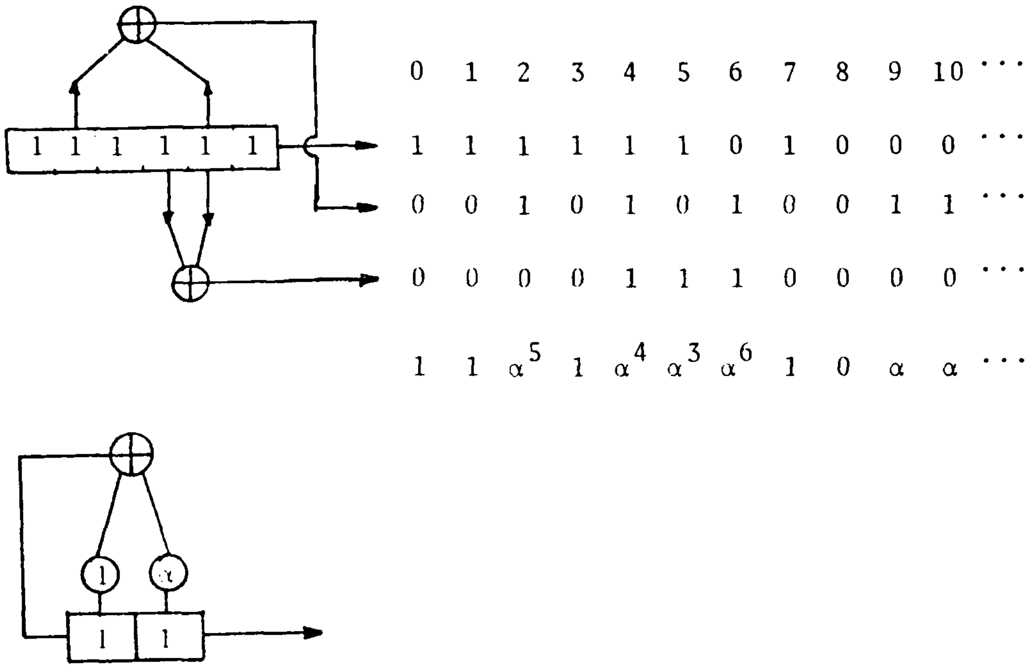


Figure 3. Implementation of an 8-state generator with a single binary feedback shift register

2.5 Construction of Tables of Irreducible Polynomials of Degree 2 over GF(2^3)

In order to illustrate the computation of useful tables of multistate irreducible polynomials, and in order to have at hand a convenient list of such polynomials to aid in the study of multistate sequences, a table of irreducible polynomials of degree 2 over the finite field GF(2^3) was constructed. These polynomials will generate eight (8) state pseudonoise sequences whose periods are factors of 63.

The multistate polynomials in each group of three (3) of Table 1 are factors of the binary polynomial in the product column. Thus, for example

$$(x^2 + \beta^3 x + \beta)(x^2 + \beta^6 x + \beta^2)(x^2 + \beta^5 x + \beta^2) = x^6 + x + 1$$

Table 1. Irreducible Polynomials of Degree 2 over $GF(2^3)$

		Period	Product
1	$x^2 + \beta^3 x + \beta$		
2	$x^2 + \beta^6 x + \beta^2$	63	$x^6 + x + 1$
4	$x^2 + \beta^5 x + \beta^4$		
3	$x^2 + \beta^5 x + \beta^3$		
6	$x^2 + \beta^3 x + \beta^6$	21	$x^6 + x^4 + x^2 + x + 1$
12	$x^2 + \beta^6 x + \beta^5$		
5	$x^2 + \beta^2 x + \beta^5$		
10	$x^2 + \beta^4 x + \beta^3$	63	$x^6 + x^5 + x^2 + x + 1$
20	$x^2 + \beta x + \beta^6$		
7	$x^2 + \beta^5 x + 1$		
14	$x^2 + \beta^3 x + 1$	9	$x^6 + x^3 + 1$
28	$x^2 + \beta^6 x + 1$		
11	$x^2 + x + \beta^4$		
22	$x^2 + x + \beta$	63	$x^6 + x^5 + x^3 + x^2 + 1$
44	$x^2 + x + \beta^2$		
13	$x^2 + \beta^6 x + \beta^6$		
26	$x^2 + \beta^5 x + \beta^5$	63	$x^6 + x^5 + x^3 + x^2 + 1$
52	$x^2 + \beta^3 x + \beta^3$		
15	$x^2 + \beta^4 x + \beta$		
30	$x^2 + \beta x + \beta^2$	21	$x^6 + x^5 + x^4 + x^2 + 1$
60	$x^2 + \beta^2 x + \beta^4$		
21	$x^2 + x + 1$	3	$x^2 + x + 1$

Table 1. Irreducible Polynomials of Degree 2 over $GF(2^3)$ - (Continued)

23	$x^2 + \beta^4 x + \beta^2$		
46	$x^2 + \beta x + \beta^4$	63	$x^6 + x^5 + x^4 + x + 1$
29	$x^2 + \beta^2 x +$		
31	$x^2 + \beta x + \beta^3$		
62	$x^2 + \beta^2 x + \beta^6$	63	$x^6 + x^5 + 1$
61	$x^2 + \beta^4 x + \beta^5$		

The roots of the polynomial $x^6 + x + 1$ are

$\{\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16}\ \alpha^{32}\}$

α and α^8 are roots of $x^2 + \beta^3 + \beta$

α^2 and α^{16} are roots of $x^2 + \beta^6 + \beta^2$ $\qquad \beta = \alpha^9$

α^4 and α^{32} are roots of $x^2 + \beta^5 + \beta^4$ $\qquad \beta^3 + \beta^2 + 1 = 0$

2.6 Some Properties of Multistate Sequences

2.6.1 Multiplication of a Multistate Sequence by a Character

The following result describes what happens when a multi-state sequence is multiplied by a character. The resulting sequence is a phase shift of the original sequence. The precise phase shift obtained is described by the following result.

Result: Suppose we have a 2^k-state maximal sequence h corresponding to the n^{th} degree polynomial $f(x) \in GF(2^k)[x]$ with root α^v in $GF(2^{k \cdot n})$. (The values taken by this sequence are $\{0, 1, \beta \ldots \beta^{2^k - 1}\}$ where $\beta = \alpha^{\frac{2^{k \cdot n} - 1}{2^k - 1}} = \alpha^M$.) Then $\beta^j\ h(i) = h(i - jv^{-1}M)$.

Proof: By previous result there exists a linear mapping ϕ of $GF(2^{k \cdot n})$ into $GF(2^k)$ such that $h(i) = \phi\left((\alpha^v)^{-i}\right)$.

$h(i - jv^{-1}M) =$

$\phi\left[(\alpha^v)^{-(i - jv^{-1}M)}\right] =$

$\phi\left[(\alpha^v)^{-i}\ (\alpha^{jM})\right] =$

$\phi\left[(\alpha^v)^{-i}\ \beta^j\right] = \beta^j\ \phi\left[(\alpha^v)^{-i}\right] = \beta^j\ h(i)$

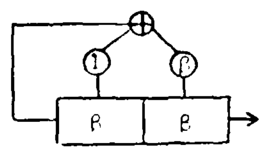
Example: (see following page)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
h =	β	β	β^6	β	β^5	β^4	1	β	0	β^2	β^2	1	β^2	β^6	β^5	β	β^2	0	β^3	β^3	β	β^3	1	β^6	β^2	β^3	0	β^4	β^4	β^2	β^4	β	1	β^3	β^4

35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	0	1	2	3	4	5	6
0	β^5	β^5	β^3	β^5	β^2	β	β^4	β^5	0	β^6	β^6	β^4	β^6	β^2	β^2	β^5	β^6	0	1	1	β^5	1	β^4	β^2	β^5	1	0	β	β	β^6	β	β^5	β^4	1

$\beta \in GF(2^3) \subset GF(2^6)$ $\quad$ β is root of $x^3 + x^2 + 1$ $\quad$ α is root of $x^6 + x + 1$ $\quad$ $\beta = \alpha^9$

$$h = \frac{1}{x^2 + \beta^6 x + \beta^6} = \beta + \beta x + \beta^6 x^3 + \ldots$$



α^{13} is a root of $x^2 + \beta^6 x + \beta^5$ $\quad$ $v = 13$ $\quad$ $v^{-1} = 34$

Thus $\beta\, h(i) = h(i - v^{-1}M) = h\Big(i - (34)(9)\Big) = h(i - 54)$

In fact

$$\beta h = \beta^2\ \beta^2\ 1\ \beta^2\ \ldots = h_{54}$$

2.6.2 Binary Representation of Maximal Multistate Sequences

Result: Suppose we have a 2^3-state maximal sequence h corresponding to the n^{th} degree polynomial $f(x) \in GF(2^3)[x]$ with root α^v in $GF(2^{3 \cdot n})$. Let $\frac{g(x)}{f(x)}$ be a rationalized representation of h. Then the binary representation of the sequence $h = \frac{g(x)}{f(x)}$ is given by

$$h = \left[\left(P_1 h\right), \left(P_1 h\right)_{-(v^{-1}M)}, \left(P_1 h\right)_{(v^{-1}M)}\right]$$

where: $M = \dfrac{2^{3n} - 1}{2^3 - 1}$.

Proof:

$$h = \left[\frac{P_1(g(x))}{f(x)}, \frac{P_2(g(x))}{f(x)}, \frac{P_3(g(x))}{f(x)}\right]$$

$$= \left[\frac{P_1(g(x))}{f(x)}, \frac{P_1\left(\beta^{-1}(g(x))\right)}{f(x)}, \frac{P_1\left(\beta(g(x))\right)}{f(x)}\right]$$

$$= \left[P_1\left(\frac{g(x)}{f(x)}\right), P_1\left((\beta^{-1})\left(\frac{g(x)}{f(x)}\right)\right), P_1\left((\beta)\left(\frac{g(x)}{f(x)}\right)\right)\right]$$

$$= \left[\left(P_1 h\right), P_1\left(h_{-(v^{-1}M)}\right), P_1\left(h_{(v^{-1}M)}\right)\right]$$

$$= \left[\left(P_1 h\right), \left(P_1 h\right)_{-(v^{-1}M)}, \left(P_1 h\right)_{v^{-1}M}\right]$$

Example: Suppose we consider the 2^3-state maximal sequence h corresponding to the 2^{nd} degree polynomial $x^2 + \alpha^6 x + \alpha^6$. The sequence generated by the polynomial and the binary representation of the sequence

have been shown in Section 2.4 to be the sequences of Figure 2. We note from Table 1 that α^{13} is a root of the polynomial $x^2 + \alpha^6 x + \alpha^6$. Thus $v = 13$; $v^{-1} = 34$ and $v^{-1}M = 54$. Thus the binary sequence representation of the 8-state sequence is

$$\left[\left(P_1 h\right), \left(P_1 h\right)_{-54}, \left(P_1 h\right)_{54}\right] = \left[\left(P_1 h\right), \left(P_1 h\right)_9, \left(P_1 h\right)_{-9}\right]$$

This may be verified by observing the binary sequence representation of Figure 2.

2.6.3 Sequences Generated by Conjugate Polynomials

The k-1 conjugate polynomial to a polynomial $f(x) \in GF(2^k)$ are obtained by replacing the coefficient $f(j)$ of x^j by $\left(f(j)\right)^2$, $\left(f(j)\right)^{2^2}$, . . . $f(j)^{2^{k-1}}$, respectively. Thus, for example, the conjugate polynomials to $x^2 + \beta^6 x + \beta^6 \in GF(2^3)[x]$ are found to be

$$1^2\, x^2 + (\beta^6)^2 x + (\beta^6)^2 = x^2 + \beta^5 x + \beta^5$$

$$1^4\, x^2 + (\beta^6)^4 x + (\beta^6)^4 = x^2 + \beta^3 + \beta^3$$

The 2^k state sequences generated by these conjugate polynomials can be obtained from the sequences h generated by the polynomial $f(x)$ by replacing each term $h(i)$ of the sequence by $\left(h(i)\right)^2$, $\left(h(i)\right)^{2^2}$, . . . $\left(h(i)\right)^{2^{k-1}}$, respectively. Thus in the above example if $h(0)$, $h(1)$, . . . is the sequence generated by $f(x) = x^2 + \alpha^6 x + \alpha^6$, then $\left(h(0)\right)^2$, $\left(h(1)\right)^2$ . . . and $\left(h(0)\right)^4$, $\left(h(1)\right)^4$, . . . will be the sequences generated by $x^2 + \alpha^5 x + \alpha^5$ and $x^2 + \alpha^3 x + \alpha^3$, respectively.

Since the j^{th} conjugate polynomial to the polynomial $f(x) \in GF(2^3)$ having root α^v has root $\alpha^{2^j v}$, the binary representation of the sequence corresponding to this conjugate polynomial is

$$h_j = \left[\left(P_1 h_j\right), \left(P_1 h_j\right)_{-(2^j v)^{-1}M}, \left(P_1 h_j\right)_{(2^j v)^{-1}M}\right]$$

$$= \left[\left(P_1 h_j\right), \left(P_1 h_j\right)_{-2^{3n-j}(v^{-1}M)}, \left(P_1 h_j\right)_{2^{3n-j}(v^{-1}M)}\right]$$

Example: The polynomial $x^2 + \beta^6 x + \beta^6$ having root α^{13} will generate the sequence $h = 1\ 1\ \beta^5\ 1\ \beta^4\ \beta^3\ \beta^6\ \ldots$. This sequence can be represented by phase shifts of a binary sequence a corresponding to the polynomial $x^6 + x^5 + x^3 + x^2 + 1 = (x^2 + \beta^6 x + \beta^6)(x^2 + \beta^5 x + \beta^5)(x^2 + \beta^3 x + \beta^3)$. In fact in Figure 2 we have

h	=	1	1	β^5	1	β^4	β^3	β^6	...
a	=	1	1	1	1	1	1	0	...
a_9	=	0	0	1	0	1	0	1	...
a_{-9}	=	0	0	0	0	1	1	1	...

The conjugate polynomial $x^2 + \beta^5 x + \beta^6$ having root α^{26} will generate the sequence $h' = 1\ 1\ \beta^6\ 1\ \beta\ \beta^6\ \beta^5\ \ldots$, which is obtained from the sequence h by replacing each term $h(i)$ by $\left(h(i)\right)^2$. The sequence h'

can be represented by phase shifts of the sequence a in accordance with the above result. Thus we have

$$
\begin{array}{ccccccccccccc}
 & & h' & = & 1 & 1 & \beta^3 & 1 & \beta & \beta^6 & \beta^5 & \dots \\
a_{18} & = & a' & = & 1 & 1 & 1 & 1 & 0 & 0 & 1 & \dots \\
a'_{32\times 9} & = & a'_{36} & = & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \dots \\
a_{-32\times 9} & = & a'_{-36} & = & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \dots
\end{array}
$$

The conjugate polynomial $x^2 + \beta^3 x + \beta^3$ having root α^{52} will generate the sequence $h'' = 1\ 1\ \beta^6\ 1\ \beta^2\ \beta^5\ \beta^3 \dots$ which is obtained from the sequence h by replacing each term $h(i)$ by $\big(h(i)\big)^4$. The sequence h'' can be represented by phase shifts of the sequence a in accordance with the above result. Thus we have

$$
\begin{array}{ccccccccccccc}
 & & h'' & = & 1 & 1 & \beta^6 & 1 & \beta^2 & \beta^5 & \beta^3 & \dots \\
a_{27} & = & a'' & = & 1 & 1 & 0 & 1 & 0 & 1 & 1 & \dots \\
a''_{16\times 9} & = & a''_{18} & = & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \dots \\
a''_{-16\times 9} & = & a''_{-18} & = & 0 & 0 & 1 & 0 & 1 & 0 & 1 & \dots
\end{array}
$$

3. CORRELATION FUNCTION OF MULTISTATE SEQUENCES

3.1 Definition of θ

The correlation function with respect to a complex valued mapping of the sequence alphabet of two (2) multi-state sequences has been defined (in Report No. 1) as follows

$$\theta_{\eta}(a,b)(\tau) = \frac{1}{P} \sum_{k=0}^{P-1} \eta\big(a(k)\big)\, \overline{\eta\big(b(k-\tau)\big)}$$

where a,b are multi-state sequences of period P

η is complex valued mapping of the sequence alphabet

In what follows, we compute the auto correlation function with respect to a specific complex valued function η of maximal multi-state PN sequences.

3.2 The Mapping of η

The specific complex valued mapping of $GF(2^k)$ which we shall use has values on the complex unit circle. The mapping η ultimately determines the correspondence between the characters of the multi-state alphabet and the phase of the carrier which will be modulated by the multi-state sequence.

Definition: η is a complex valued mapping of

$$GF(2^k) = \left\{0,\ 1,\ \beta,\ \beta^2\ \ldots\ \beta^{2^k-2}\right\} \quad \text{given by}$$

$$\eta(0) = 1$$

$$\eta(\beta^s) = e^{\frac{i(s+1)\pi}{2^{k-1}}} \qquad 0 \le s \le 2^k - 2$$

We note that

$$\eta(\beta^s) = e^{\frac{i(s+2)\pi}{2^{k-1}}} \qquad 2^k - 1 \le s \le 2^{k+1} - 3$$

Example: $GF(2^3) = 0, 1, \beta', \ldots \beta^6$

$$\eta(0) = 1$$

$$\eta(\beta^0) = e^{\frac{i\pi}{4}} = \frac{\sqrt{2}}{2} + i\,\frac{\sqrt{2}}{2}$$

$$\eta(\beta^1) = e^{\frac{i2\pi}{4}} = 0 + i$$

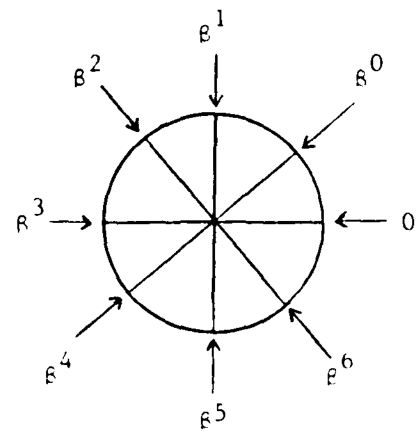
$$\eta(\beta^2) = e^{\frac{i3\pi}{4}} = -\frac{\sqrt{2}}{2} + i\,\frac{\sqrt{2}}{2}$$

$$\eta(\beta^3) = e^{\frac{i4\pi}{4}} = -1 + i\,0$$

$$\eta(\beta^4) = e^{\frac{i5\pi}{4}} = -\frac{\sqrt{2}}{2} - i\,\frac{\sqrt{2}}{2}$$

$$\eta(\beta^5) = e^{\frac{i6\pi}{4}} = 0 - i$$

$$\eta(\beta^6) = e^{\frac{i7\pi}{4}} = \frac{\sqrt{2}}{2} - i\,\frac{\sqrt{2}}{2}$$



3.3 Computation of the Autocorrelation Function of Multistate Maximal Sequences

Result: Suppose we have a 2^k-state maximal sequence a corresponding to the n^{th} degree polynomial $f(x) \in GF(2^k)[x]$ with root α^v in $GF(2^{k\cdot n})$. The values taken by this sequence are $\left\{0, 1, \beta \ldots \beta^{2^k-1}\right\}$ where

$\beta = \alpha^{\frac{2^{k\cdot n}-1}{2^k-1}} = \alpha^M$. The auto correlation function $\theta(a,a)$ is given by

$$\theta(a,a)((\tau)) = \left(2^k-1-vj\right) 2^{k(n-1)} e^{\frac{-ivj\pi}{2^{k-1}}} + (vj)\, 2^{k(n-1)} e^{\frac{-i(vj+1)\pi}{2^{k-1}}} + 2^{k(n-1)} - 1$$

for $\tau = jM$

$$\theta(a,a)(\tau) = -1 \qquad \text{otherwise}$$

$$\theta(a,a)(\tau) = \sum_{t=0}^{2^{n\cdot k}-1} \eta\big(a(t)\big)\,\overline{\eta\big(a(t-\tau)\big)} \qquad \text{definition of } \theta$$

$$\theta(a,a)(jM) \qquad M = \frac{2^{k\cdot n}-1}{2^k-1}$$

$$\sum_{t=0}^{2^{n\cdot k}-1} \eta\big(a(t)\big)\,\overline{\eta\big(a(t-jM)\big)}$$

$$\sum_{t=0}^{2^{n\cdot k}-1} \eta\big(a(t)\big)\,\overline{\eta\, a\big(t-(jv)(v^{-1}M)\big)}$$

$$\sum_{t=0}^{2^{n\cdot k}-1} \eta\big(a(t)\big)\,\overline{\eta\big(\beta^{jv}\, a(t)\big)} \qquad \text{previous result \# (3.0)}$$

For each non-zero term $a(t) \in GF(2^k)$ of the multi-state sequence a there is an integer $\ell\big(a(t)\big)$ where $0 \le \ell\big(a(t)\big) \le 2^k-2$. Such that $a(t) = \beta^{\ell\left(a(t)\right)}$. Thus we have

$$\sum_{\substack{t=0 \\ a(t)\neq 0}}^{2^{n\cdot k}-1} \eta\Big(\beta^{\ell(a(t))}\Big)\,\overline{\eta\Big(\beta^{jv+\ell(a(t))}\Big)} + 2^{k\cdot(n-1)} - 1$$

$$= \sum_{\substack{a(t)\neq 0 \\ jv+\ell(a(t)) \le 2^k-2}}^{2^{n\cdot k}-1} \left[e^{\frac{i\left(\ell(a(t))+1\right)\pi}{2^{k-1}}}\right]\left[e^{-\frac{i\left(\ell(a(t))+vj+1\right)\pi}{2^{k-1}}}\right]$$

$$+ \sum_{\substack{a(t)\neq 0 \\ jv+\ell(a(t)) > 2^k-2}}^{2^{n\cdot k}-1} \left[e^{\frac{i\left(\ell(a(t)) + 1\right)\pi}{2^{k-1}}}\right]\left[e^{-\frac{i\left(\ell(a(t)) + vj + 2\right)\pi}{2^{k-1}}}\right] + 2^{k(n-1)} - 1$$

$$= \sum_{\substack{a(t)\neq 0 \\ \ell(a(t)) \leq 2^k-2-j}}^{2^{n\cdot k}-1} \left[e^{-\frac{ivj\pi}{2^{k-1}}}\right] + \sum_{\substack{a(t)\neq 0 \\ \ell(a(t)) > 2^k-2-vj}}^{2^{n\cdot k}-1} \left[e^{-\frac{i(vj+1)\pi}{2^{k-1}}}\right] + 2^{k(n-1)} - 1$$

Since there are $(2^k-1) - vj$ values for which $\ell(a(t)) \leq 2^k - 2 - vj$, and there are vj values for which $\ell(a(t)) > 2^k - 2 - vj$, and since each value occurs in the sequence $2^{k(n-1)}$ times, we have

$$\theta(a,a)(jM) = \left(2^k-1-vj\right)2^{k(n-1)} e^{-\frac{ivj\pi}{2^{k-1}}} + (vj)\, 2^{k(n-1)} e^{-\frac{i(vj+1)\pi}{2^{k-1}}} + 2^{k(n-1)} - 1$$

3.4 Autocorrelation Function for 8-State Maximal Sequences

For 8-state maximal sequences, the above correlation formula becomes

$$\theta\left(j\,\frac{2^{3n}-1}{2^3-1}\right) = (7 - vj)\, 2^{3(n-1)} e^{-\frac{ivj\pi}{4}} + (vj)\, 2^{3(n-1)} e^{-\frac{i(vj+1)\pi}{4}} + 2^{3(n-1)} - 1$$

For a two-stage maximal register which generates an eight-state sequence of period 63 ($n = 2$), the correlation formula becomes

$$\theta(9j) = (7 - vj)\, 8\, e^{-\frac{ivj\pi}{4}} + vj\, 8\, e^{-\frac{i(vj+1)\pi}{4}} + 7$$

Example: We use the above formula to compute the auto correlation function of the maximal 8-state pseudo noise sequence corresponding to the polynomial $x^2 + \alpha^4 x + \alpha^2$. We note from Table 2-1 that α^{23} is a root of this polynomial. We thus have

$$\theta(9j) = (7 - 2j)(8)\, e^{-\frac{i2j\pi}{4}} + (2j)(8)\, e^{-\frac{(2j+1)\pi}{4}} + 7$$

$$\theta(9) = (5)(8)\, e^{-\frac{i2\pi}{4}} + (16)\, e^{-\frac{i3\pi}{4}} + 7 = (7 - 8\sqrt{2}) + i(-40 - 8\sqrt{2})$$

$$\theta(18) = (3)(8)\, e^{-\frac{i4\pi}{4}} + (32)\, e^{-\frac{i5\pi}{4}} + 7 = (-17 - 16\sqrt{2}) + i\ 16\sqrt{2}$$

$$\theta(27) = (1)(8)\, e^{-\frac{i6\pi}{4}} + (6)(8)\, e^{-\frac{i7\pi}{4}} + 7 = (7 + 24\sqrt{2}) + i(8 + 24\sqrt{2})$$

$$\theta(36) = (6)(8)\, e^{-\frac{i\pi}{4}} + (1)(8)\, e^{-\frac{i2\pi}{4}} + 7 = (7 + 24\sqrt{2}) + i(-8 - 24\sqrt{2})$$

$$\theta(45) = (4)(8)\, e^{-\frac{i3\pi}{4}} + (3)(8)\, e^{-\frac{i4\pi}{4}} + 7 = (-17 - 16\sqrt{2}) + i(-16\sqrt{2})$$

$$\theta(54) = (2)(8)\, e^{-\frac{i5\pi}{4}} + (5)(8)\, e^{-\frac{6\pi}{4}} + 7 = (7 - 8\sqrt{2}) + i(40 + 8\sqrt{2})$$

Example: We use the above formula to compute the auto correlation function of the maximal 8-state pseudo noise sequence corresponding to the polynomial $x^2 + \beta^4 x + \beta^2$. We note from Table 1 that α^{23} is a root of this polynomial. We thus have

$$\theta(9j) = (7 - 2j)(8)\, e^{-\frac{i2j\pi}{4}} + (2j)(8)\, e^{-\frac{i(2j+1)\pi}{4}} + 7$$

$$\theta(9) = (5)(8)\, e^{-\frac{i2\pi}{4}} + 16\, e^{-\frac{i3\pi}{4}} + 7 = (7 - 8\sqrt{2}) + i(-40 - 8\sqrt{2}) = \left(-4 \cdot 31 - i(51 \cdot 31)\right)$$

$$\theta(18) = (3)(8)\, e^{-\frac{i4\pi}{4}} + 32\, e^{-\frac{i5\pi}{4}} + 7 = (-17 - 16\sqrt{2}) + i(16\sqrt{2} = (-39 \cdot 63 + i\ 22 \cdot 63)$$

$$\theta(27) = (1)(8)\, e^{-\frac{i6\pi}{4}} + (6)(8)\, e^{-\frac{i7\pi}{4}} + 7 = (7 + 24\sqrt{2}) + i(8 + 24\sqrt{2}) = (40 \cdot 94 + i\ 41 \cdot 94)$$

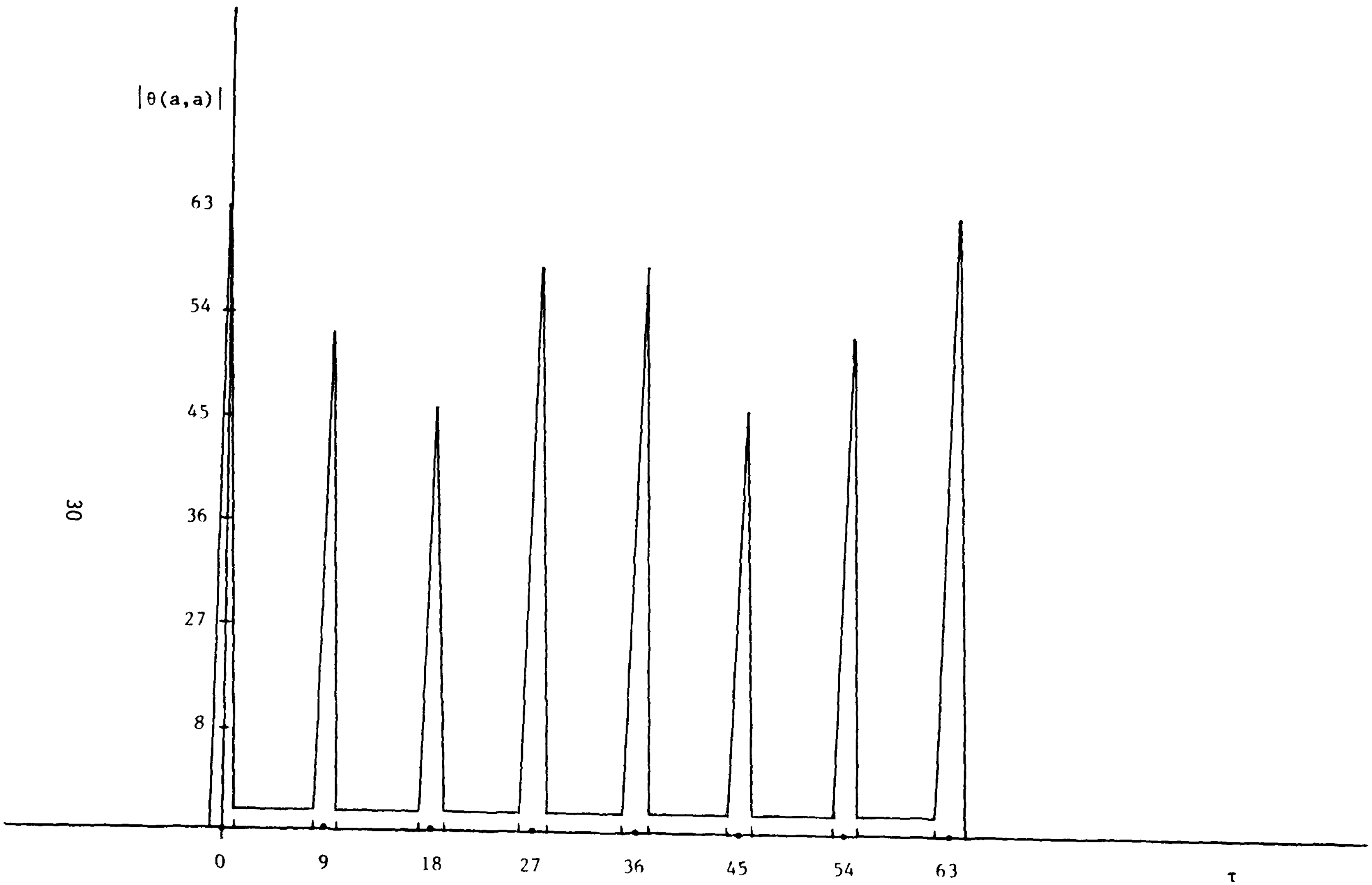


Figure 4. Absolute Value of Autocorrelation Function of Maximal Linear Sequence of Period 63 over $GF(2^3)$ $x^2 + \beta^4 x + \beta^2$

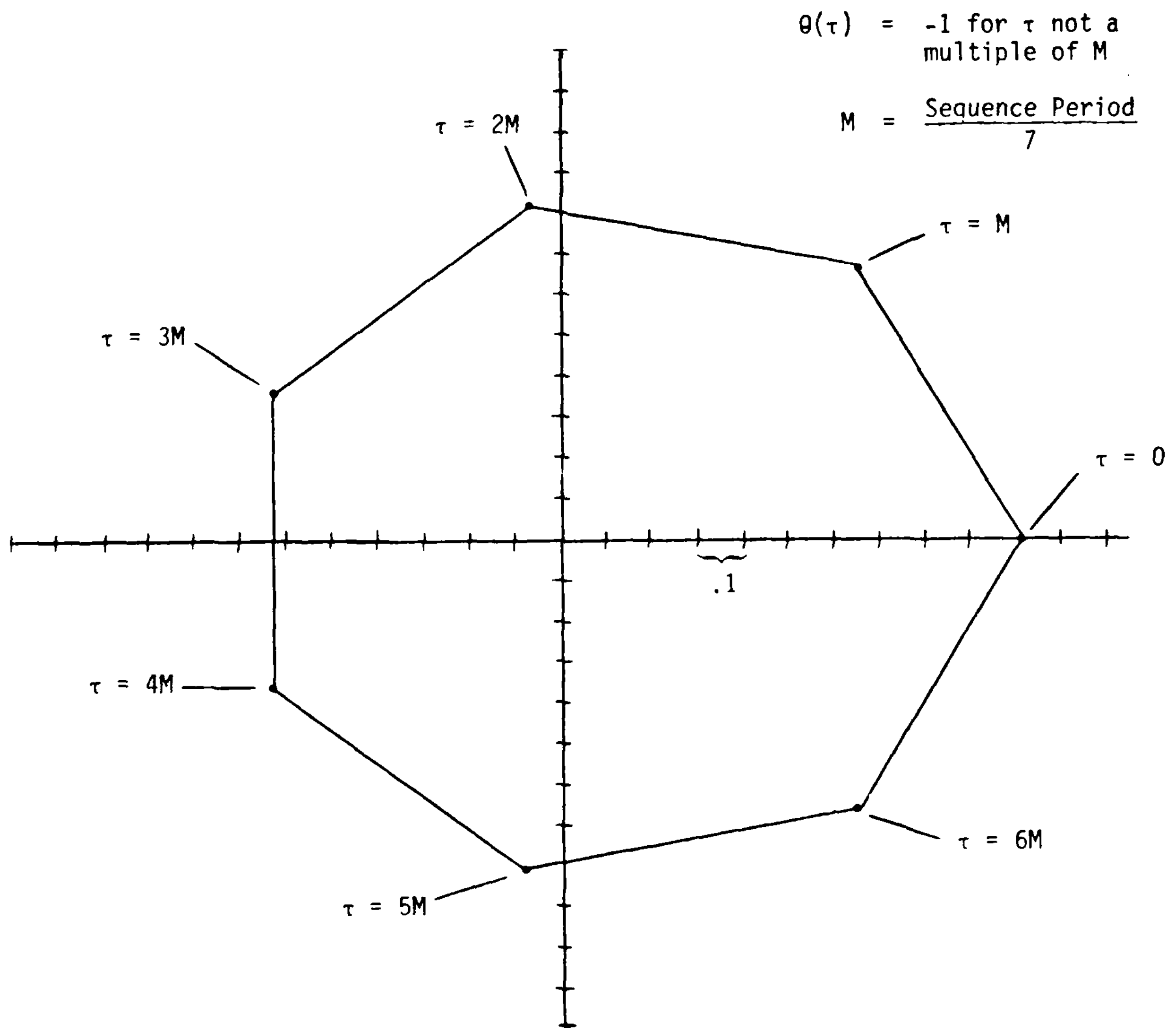


Figure 5. Autocorrelation Function of Maximal Linear Sequence over $GF(2^3)$ (Eight State)

$$\theta(36) = (6)(8)\,e^{-\frac{i\pi}{4}} + (1)(8)\,e^{-\frac{i2\pi}{4}} + 7 = (7 + 24\sqrt{2}) + i(-8 - 24\sqrt{2}) = (40 \cdot 94 - i\ 41 \cdot 94)$$

$$\theta(45) = (4)(8)\,e^{-\frac{i3\pi}{4}} + (3)(8)\,e^{-\frac{i4\pi}{4}} + 7 = (-17 - 16\sqrt{2}) + i(-16\sqrt{2}) = (-39 \cdot 63 - i\ 22 \cdot 63)$$

$$\theta(54) = (2)(8)\,e^{-\frac{i5\pi}{4}} + (5)(8)\,e^{-\frac{i6\pi}{4}} + 7 = (7 - 8\sqrt{2}) + i(40 + 8\sqrt{2}) = -4 \cdot 31 + i\ 51 \cdot 31$$

A plot of the absolute value $|\theta(a,a)|$ is presented in Figure 4, and of $\theta(a,a)$ in Figure 5.

3.5 Computation of the Autocorrelation Function of 16-State Maximal Linear Sequences

In this section we give examples of the computation of the autocorrelation function of a 16-state maximal linear sequence. The unnormalized autocorrelation function of a 2^k-state maximal linear sequence of period $2^{k \cdot n} - 1$ has been shown to be given by the formula:

$$\theta(a,a)(jM) = 2^{k(n-1)}\, Q_k(rj) - 1$$

$$\theta(a,a)(\tau) = -1 \qquad \tau \neq jM$$

where $$M = \frac{2^{k \cdot n} - 1}{2^k - 1} = \frac{\text{Sequence Period}}{(\text{No. of Sequence States}) - 1} = \text{No. of Correlation Peaks}$$

and $$Q_k(j) = \left[\left(2^k - 1 - j\right) e^{-\frac{i\,j\,\pi}{2^{k-1}}} + j\, e^{-\frac{i(j+1)\pi}{2^{k-1}}} + 1\right]$$

$$Q_4(j) = \left[(15 - j - 1)\, e^{-\frac{i\,j\,\pi}{8}} + j\, e^{-\frac{i(j+1)\pi}{8}} + 1\right]$$

j	$Q_4(j)$
1	14.6 - i 6.1
2	11.0 - i 11.0
3	5.6 - i 14.1
4	- 0.5 - i 14.7
5	- 6.4 - i 12.8
6	-10.9 - i 8.7
7	-13.4 - i 3.1
8	-13.4 + i 3.1
9	-10.9 + i 8.7
10	- 6.4 + i 12.8
11	- 0.5 + i 14.7
12	5.6 + i 14.1
13	10.9 + i 11.0
14	14.6 + i 6.1

The above values of Q_4 determine the auto correlation function of 16-state maximal linear sequences of any period. Thus, for example, for n = 2, period 255 we have:

j	$\theta(17J) = 16\ Q_4(j) - 1$	$\lvert\theta(17j)\rvert$	$\lvert\theta(17j)\rvert/255$
1	232.6 - i 97.6	252.2	.99
2	175.0 - i 176.0	248.2	.97
3	88.6 - i 225.6	242.4	.95
4	- 9.0 - i 235.2	235.4	.92
5	-103.4 - i 204.8	229.4	.90
6	-175.4 - i 139.2	224.0	.88
7	-215.4 - i 49.6	221.0	.87
8	-215.4 + i 49.6	221.0	.87
9	-175.4 + i 139.2	224.0	.88
10	-103.4 + i 204.8	229.4	.90
11	- 9.0 + i 235.2	235.4	.92
12	88.6 + i 225.6	242.4	.95
13	175.0 + i 176.0	248.2	.97
14	232.6 + i 97.6	252.2	.99

The absolute values of θ are plotted in Figure 6.

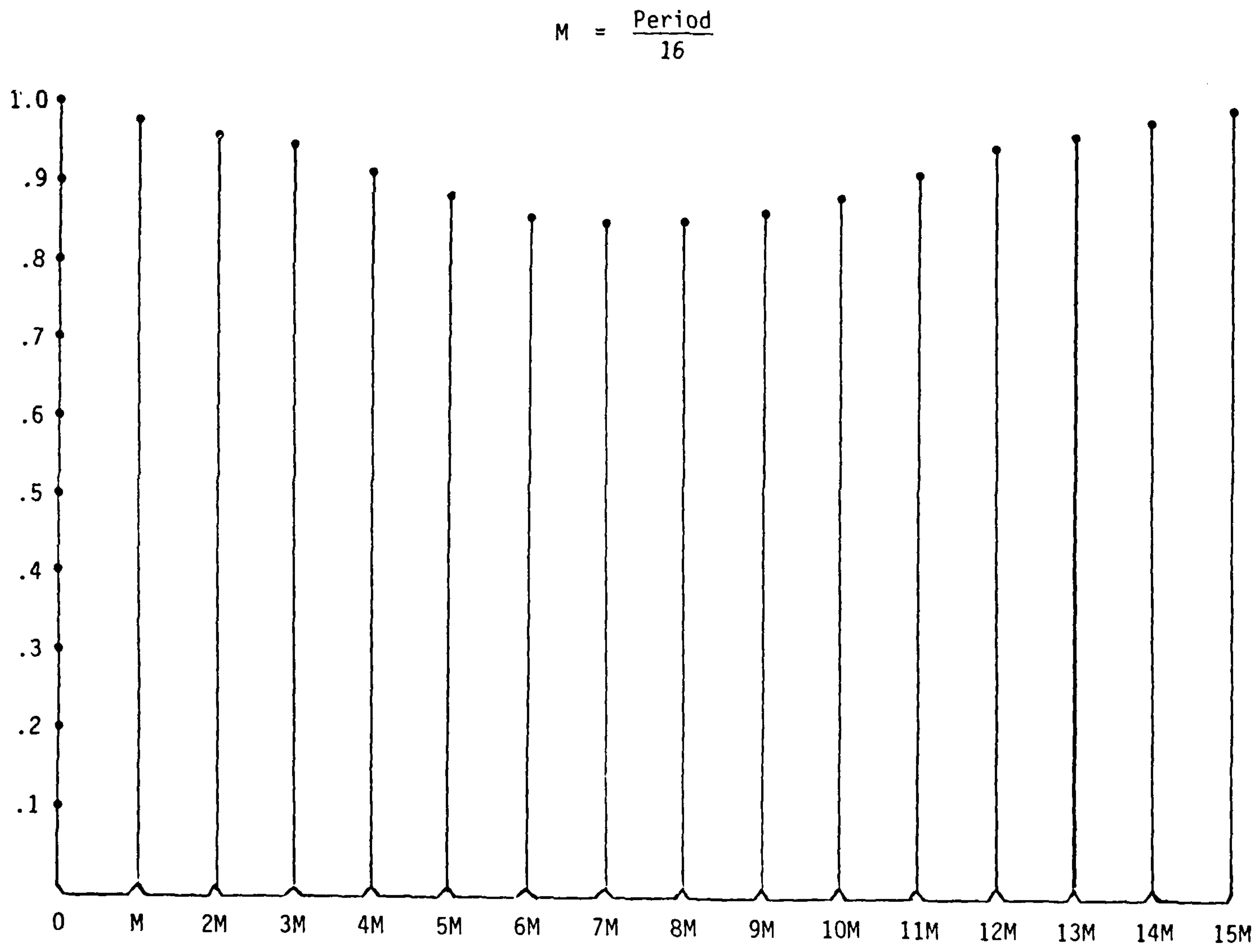


Figure 6. Absolute Value of Autocorrelation Function of Maximal Linear Sequences over $GF(2^4)$

The expression for the normalized auto correlation function is:

$$\theta(a,a)(jM) = \frac{2^{k(n-1)}\left[Q_k(rj)\right] - 1}{2^{kn} - 1}$$

This expression may be approximated by:

$$\theta(a,a)(jM) \sim \frac{Q_K(rj)}{2^k}$$

We note that this expression is independent of n.

3.6 Asymtotic Expression for θ_k

The absolute value of the normalized auto correlation peaks of multi-state maximal linear sequences approach 1 as the number of states increases. In fact we have:

$$\left|\frac{\theta(jM)}{\theta(0)}\right| \longrightarrow 1 \quad \text{for large } k$$

Proof:

$$\left|\frac{\theta(jM)}{\theta(0)}\right| = \frac{|Q_k(j)|}{2^k}$$

$$= \frac{\left|\left(2^k - 1 - j\right) e^{-\frac{i j \pi}{2^{k-1}}} + j e^{-\frac{i(j+1)\pi}{2^{k-1}}} + 1\right|}{2^k}$$

$$\frac{\left|\left(2^{k}-1\right)e^{-\frac{ij\pi}{2^{k-1}}}-j\,e^{-\frac{ij\pi}{2^{k-1}}}+j\,e^{-\frac{ij\pi}{2^{k-1}}}e^{-\frac{i\pi}{2^{k-1}}}+1\right|}{2^{k}}$$

$$\frac{\left|\left(2^{k}-1\right)e^{-\frac{ij\pi}{2^{k-1}}}-j\,e^{-\frac{ij\pi}{2^{k-1}}}\left[1-e^{-\frac{i\pi}{2^{k-1}}}\right]+1\right|}{2^{k}} \longrightarrow 1$$

3.7 Use of Correlation Sidelobes for Signal Acquisition

In this section we describe how the out-of-phase correlation sidelobes of a multi-state maximal linear sequence may be used as a synchronization aid. We show that the time required for the synchronization of multi-state sequences is significantly less than that required for the synchronization of binary maximal linear sequences.

The conventional synchronization techniques for binary sequences compares the received code with successive phase shifts of a locally generated replica of the received code until phase synchronism of the two (2) codes is achieved. If the codes have period N and the integration is carried out over W code chips for each phase comparison, then this synchronization process will require integration over as many as WN chips.

The suggested technique for the synchronization of multi-state maximal linear codes makes use of their relatively high and regularly positioned auto correlation sidelobes. The synchronization procedure uses the conventional search technique to locate one of the set of equally spaced correlation sidelobes. Since the auto correlation sidelobes are spaced M chips apart, at most M relative phase shifts of the two (2) codes must be compared in order

to find one of the auto correlation sidelobes. The location of one of the auto correlation peaks determines the phase position of the other $\frac{N}{M}$ regularly spaced correlation peaks. Each of these phase positions is then tested to determine phase synchronism between the received and locally generated codes.

Since the correlation sidelobes which are being searched out in this procedure have a normalized value θ of less than one, the integration process must be taken over a greater number of code chips in order to compensate for the fact that the two (2) code phases being compared are not perfectly correlated. Thus if the integration is performed for time T in the case of perfect correlation ($\theta = 1$), then the integration time must be $T_1 = \frac{T}{\theta^2}$ in order to obtain an equivalent amount of energy out of the correlator. The following argument established this fact.

Suppose that in the case of perfect correlation the voltage out of the correlator is V or equivalently the normalized power is V^2. If we integrate over a time T, we obtain an energy level of $E = V^2T$. If the normalized correlation function θ is less than one, then the voltage at the output of the correlator is θV or equivalently the normalized power is $(\theta V)^2$. In order to obtain the same signal energy at the output of the correlator as in the previous case, we must integrate over a time T, such that $(\theta V)^2 T_1 = V^2 T$ or $T_1 = \frac{T}{\theta^2}$.

We now compare the acquisition times required for binary and multi-state maximal linear sequences. We assume that the binary sequence is acquired by integrating over W chips in each relative phase position so that the acquisition process will require integration over as many as WN chips, where W is the code period. To acquire a multi-state maximal linear sequence, we first find one of the $\left(\frac{N}{M}\right)$ correlation peaks. The maximum number of chips over which

we must integrate is $M\left(\frac{W}{\theta^2}\right)$ chips. The maximum number of chips over which we must integrate to find the mean correlation peak is $\left(\frac{N}{M}\right)\frac{W}{(1-\theta)^2}$. Thus the total maximum number of chips over which we must integrate is $\frac{WM}{\theta^2}+\left(\frac{N}{M}\right)\frac{W}{(1-\theta)^2}$. The ratio of this number of chips to the maximum number of chips WN over which we must integrate to acquire a binary maximal linear sequence is

$$\alpha = \left(\frac{M}{N}\right)\frac{1}{\theta^2}+\frac{1}{M}\ \frac{1}{(1-\theta)^2}$$

For maximal 2^k-state sequences $N = 2^{k\cdot n}-1$ and $M = \frac{2^{k\cdot n}-1}{2^k-1}$. The above formula thus becomes

$$\alpha = \left(\frac{2^{k\ n}-1}{2^k-1}\right)\left(\frac{1}{2^{k\ n}-1}\right)\left(\frac{1}{\theta^2}\right) + \left(\frac{2^k-1}{2^{k\ n}-1}\right)\left(\frac{1}{(1-\theta)^2}\right)$$

For 8-state maximal linear sequences we have

$$\alpha = \frac{1}{7\theta^2}+\frac{7}{\left(2^{3\ n}-1\right)(1-\theta)^2}$$

Using the average value of θ over the six (6) auto correlation sidelobes, we have $\overline{\theta} = \cdot 83$

$$\alpha = \cdot 21 + \frac{243}{2^{3\cdot n}-1}$$

This function is plotted in Figure 7.

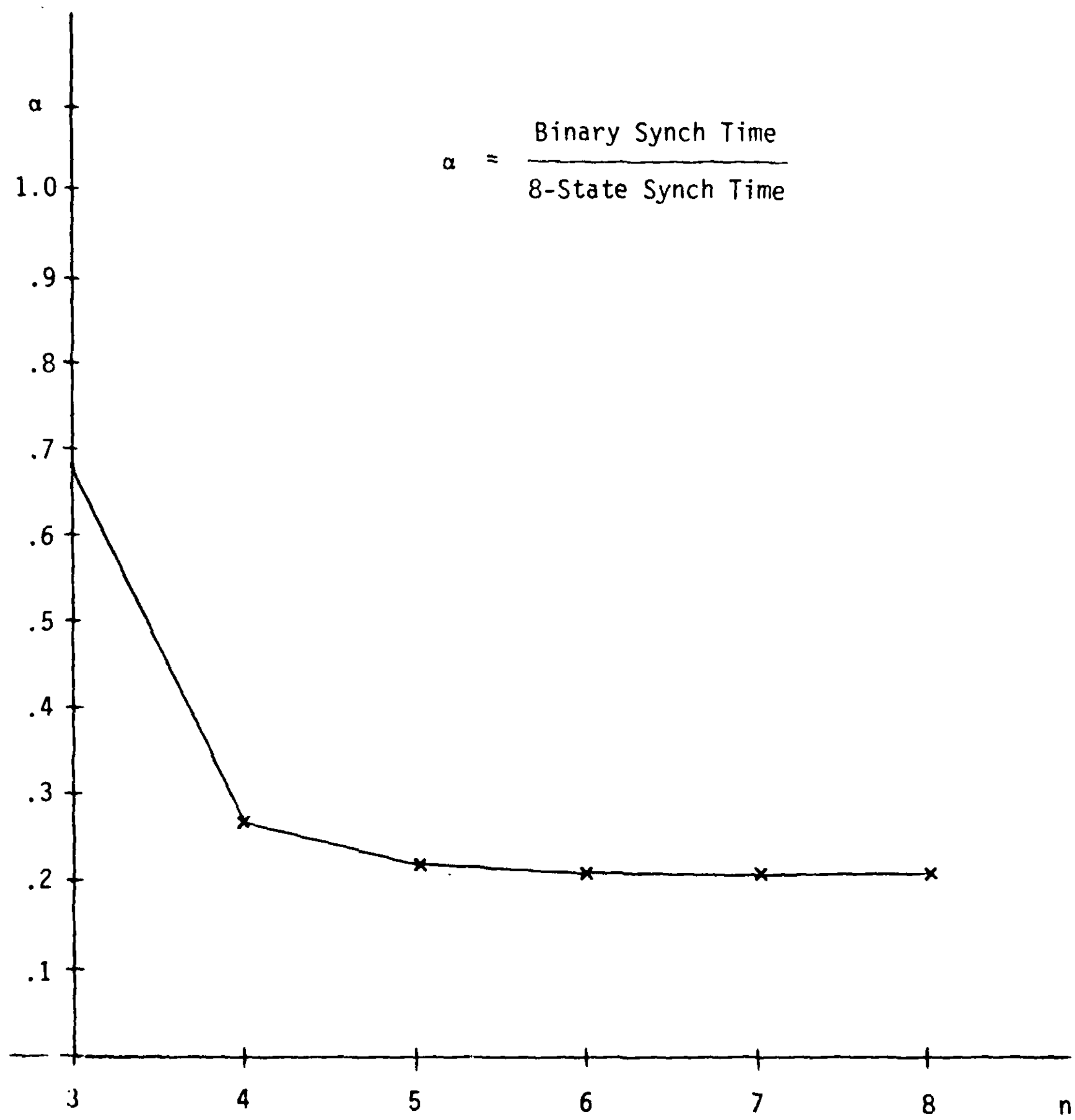


Figure 7. Comparison of Binary and Multistate Synchronization Times

3.8 Power Spectral Density of a Maximal Linear Sequence over GF(2^k)

In this section we determine the power spectral density of a maximal linear sequence over GF(2^k) in terms of the complex valued Q-function which has been defined as

$$Q_k(j) = \left(2^k - 1 - j\right)\omega^{-j} + j\omega^{-(j+1)} + 1 \qquad \text{where } \omega = e^{\frac{2\pi i}{2^k}}$$

The power spectral density S of a maximal linear sequence over GF(2^k) will be

$$\boxed{\begin{aligned} S(o) &= 1 \\ S(j) &= (P+1)\,\frac{F(Q_k)(j)}{2^k} \\ \text{where } F(Q_k)(j) &= \sum_{s=0}^{2^k-2} Q_k(s)\, e^{-\frac{2\pi i j s}{2^k - 1}} \end{aligned}}$$

The form of the autocorrelation function and power spectral density of a maximal linear sequence is illustrated in Figure 8.

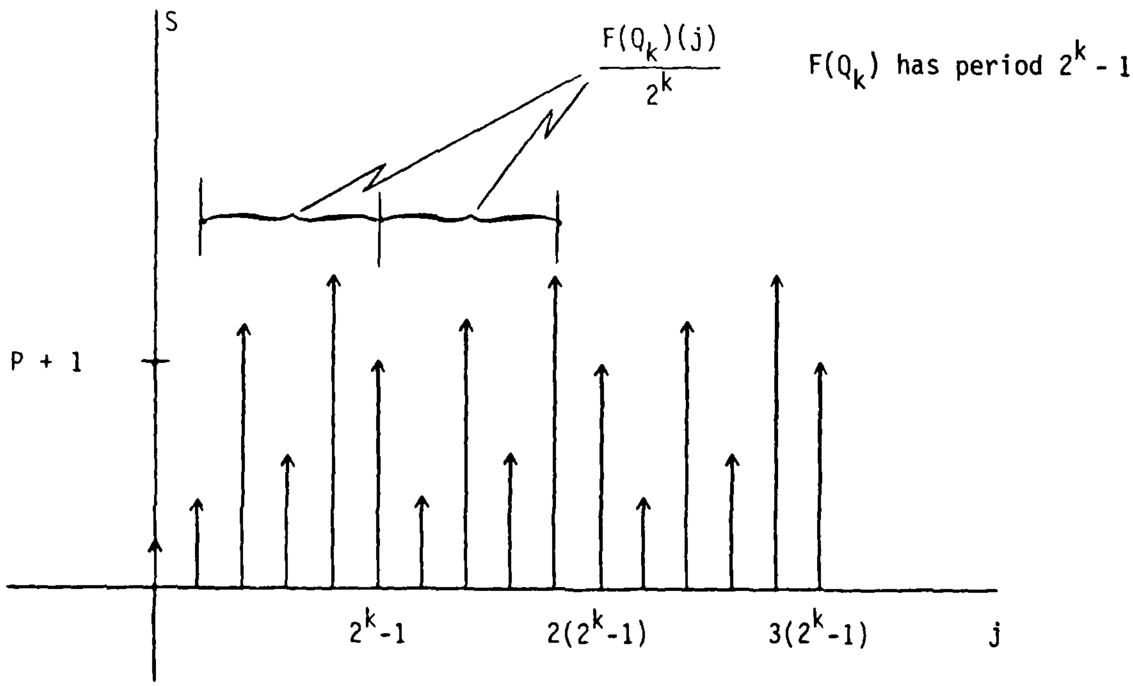


Figure 8. Power Spectral Density of Maximal Linear Sequence over GF(2^k)

The power spectral density S of a sequence a of period P is found via the Weiner Khinchin Theorem by taking the discrete Fourier transform F of its autocorrelation function θ where the Fourier transform is given by

$$S(a)(j) = F(\theta(a))(j) = \sum_{k=0}^{P-1} \theta(a)(k)\, e^{-\frac{2\pi ijk}{P}}$$

In this section we show that if a is a maximal linear sequence of period $P = 2^{n\cdot k} - 1$, then

$$S(a)(o) = 1$$

$$S(a)\left(j(2^k - 1)\right) = 2^{kn} = P + 1$$

$$S(a)(j) = 2^{k(n-1)} F(Q_k)(j) \qquad \text{for } j \text{ is not a multiple of } 2^k - 1$$

We first make the following computation for Q_k

Result: Let $Q_k(j) = (2^k - 1 - j)\,\omega^{-j} + j\,\omega^{-(j+1)} + 1 \qquad \omega = e^{\frac{2\pi i}{2^k}}$

$$\text{Then } \sum_{j=0}^{2^k-2} Q_k(j) = 2^k$$

Proof: $$\sum_{j=0}^{2^k-2} X^j = \frac{1 - X^{2^k-1}}{1 - X} = \frac{X^{2^k} - X^{2^k-1} - X + 1}{(1 - X)^2}$$

Differentiating and multiplying by X we have the identity

$$\sum_{j=0}^{2^k-2} j\,X^j = \frac{(2^k-2)X^{2^k} - (2^k-1)X^{2^k-1} + X}{(1 - X)^2}$$

Using these identities with $X = \omega$ we obtain

$$(1) \quad (2^k - 1) \sum_{j=0}^{2^k-2} \omega^j = \frac{2(2^k-1) - (2^k-1)\omega^{-1} - (2^k-1)\omega}{(1-\omega)^2}$$

$$(2) \quad - \sum_{j=0}^{2^k-2} j\,\omega^j = - \frac{(2^k-2) + (2^k-1)\omega^{-1} - \omega}{(1-\omega)^2}$$

$$(3) \quad \sum_{j=0}^{2^k-2} j\,\omega^{j+1} = \frac{(2^k-2)\omega - (2^k-1) + \omega^2}{(1-\omega)^2}$$

(1) + (2) + (3) = 1, and hence the result follows.

We now compute $S(a)$

Proof: $$S(a)(j) = F(\theta)(j) = \sum_{s=0}^{P-1} \theta(s)\, e^{-\frac{2\pi i j s}{P}} \qquad P = 2^{nk} - 1$$

Let θ' be the autocorrelation function of a binary maximal linear sequence of period $2^{n\cdot k} - 1$. It is well known that

$$\theta'(0) = 2^{n\cdot k} - 1 \qquad F(\theta')(0) = 1$$

and

$$\theta'(s) = -1 \text{ for } s \neq 0 \qquad F(\theta')(j) = P + 1 = 2^{k\cdot n} \text{ for } j \neq 0$$

Since $\theta(s) = -1$ for s, not a multiple of $M = \frac{2^{n \cdot k} - 1}{2^k - 1}$, we have

$$\sum_{s=0}^{P-1} \theta(s)\, e^{-\frac{2\pi ijs}{P}} =$$

$$\sum_{s=0}^{P-1} \theta'(s)\, e^{-\frac{2\pi ijs}{P}} + \sum_{s=1}^{2^k-2} [1 + \theta(sM)]\, e^{-\frac{2\pi ijMs}{P}}$$

$$\sum_{s=0}^{P-1} \theta'(s)\, e^{-\frac{2\pi ijs}{P}} + \sum_{s=1}^{2^k-2} [1 + \theta(sM)]\, e^{-\frac{2\pi i s}{2^k - 1}}$$

Since $\theta(sM) = 2^{k(n-1)} Q_k(j) - 1$, we have

$$\sum_{s=0}^{P-1} \theta'(s)\, e^{-\frac{2\pi ijs}{P}} + 2^{k(n-1)} \sum_{s=1}^{2^k-2} Q_k(s)\, e^{-\frac{2\pi ijs}{2^k-1}}$$

Since $Q_k(0) = 2^k$, we have

$$\sum_{s=0}^{P-1} \theta'(k)\, e^{-\frac{2\pi ijs}{P}} + 2^{k(n-1)} \sum_{s=0}^{2^k-2} Q_k(s)\, e^{-\frac{2\pi ijs}{2^k-1}} - 2^{k \cdot n}$$

$$= F(\theta')(j) + 2^{k(n-1)} F(Q_k)(j) - 2^{k \cdot n}$$

Since $F(\theta')(0) = 1$ and $F(Q_k)(0) = 2^k$, we have

$$S(a)(0) = 1$$

$$F(\theta')(j) = P + 1 = 2^{k \cdot n} \quad \text{for} \quad j \neq 0. \text{ Hence}$$

$$S(a)(j) = 2^{k(n-1)} F(Q_k)(j) \quad \text{for} \quad j \neq 0$$

$$F(Q_k)\left(j(2^k-1)\right) = \sum_{s=0}^{2^k-2} Q_k(s) = 2^k$$

Thus $$S(a)\left(j(2^k-1)\right) = 2^{kn} = P + 1.$$

The power spectral density of a maximal linear sequence of period 63 is shown in Figure 9.

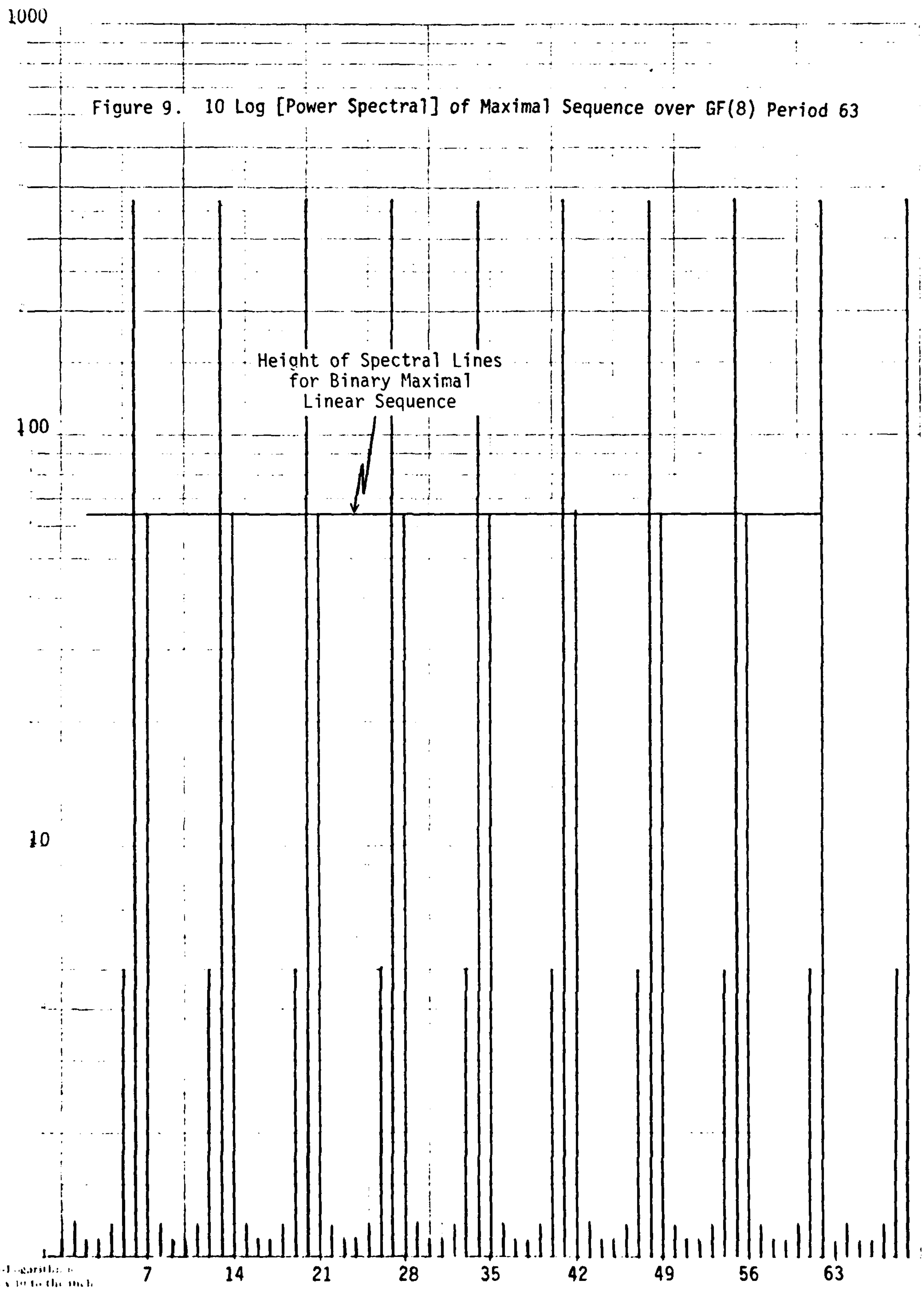


Figure 9. 10 Log [Power Spectral] of Maximal Sequence over GF(8) Period 63

APPENDIX A

Theorem: Let ϕ be any linear mapping of the field $GF(2^n)$ into the field $GF(2^k)$. Let f be any polynomial with coefficients in $GF(2^k)$, i.e., $f \in GF(2^k)[x]$. Let α be a root of f in $GF(2^n)$. The sequence $h(i) = \phi(\alpha^{-i})$ is a member of V(f), i.e., the sequence h can be generated by the shif· register corresponding to the polynomial f.

Proof: We assert that the sequence

$$h(i) = \phi(\alpha^{-i})$$

can be generated by the shift register corresponding to the polynomial f(x) where $f(\alpha) = 0$. The sequences h generated by the polynomial f(x) are those which satisfy the recursion relation:

$$f(0)h(i) = f(1)h(i-1) + f(2)h(i-2) + \ldots f(n)h(i-n) \qquad \text{for all } i \geq n$$

Thus, to show that the sequence h can be generated by the polynomial f, we must show that is satisfies the recursion relation.

$$f(\alpha) = 0$$

hence $\quad f(0) + f(1)\alpha + f(2)\alpha^2 + \ldots f(n)\alpha^n = 0$

multiplying by α^{-i} we have

$$f(0)\alpha^{-i} + f(1)\alpha^{-(i-1)} + f(2)\alpha^{-(i-2)} + \ldots f(n)\alpha^{-(i-n)} = 0$$

$$\phi\left(f(0)\alpha^{-i} + f(1)\alpha^{-(i-1)} + \ldots f(n)\alpha^{-(i-n)}\right) = \phi(0) = 0$$

$$f(0)\phi(\alpha^{-i}) + f(1)\phi\left(\alpha^{-(i-1)}\right) + \ldots f(n)\phi\left(\alpha^{-(i-n)}\right) = 0$$

$$f(0)h(i) + f(1)h(i-1) + \ldots f(n)h(i-n) = 0$$

Theorem: (Converse) Given any 2^k-state sequence h with values in $GF(2^k)$ which has been generated by a shift register corresponding to the irreducible polynomial $f(x)$ of degree n and having coefficients in $GF(2^k)$, then there is a linear mapping ϕ of $GF(2^n)$ into $GF(2^k)$ such that $h(i) = \phi(\alpha^{-i})$ where α is a root of $f(x)$.

APPENDIX B

In this appendix we review the properties of the projection mapping [1].

Result: For all $\gamma \in GF(2^3)$ we have

$$P_2(\gamma) = P_1\left(\beta^{-1}\gamma\right)$$
$$P_3(\gamma) = P_1(\beta\gamma)$$

Proof:

$$\gamma = a(0) + a(1)\beta + a(2)\beta^2$$

$$\beta\gamma = a(0)\beta + a(1)\beta + a(2)(\beta^2 + 1)$$

$$= a(2) + a(0)\beta + \left(a(1) + a(2)\right)\beta^2$$

$$\beta^{-1}\gamma = a(0)\beta^6 + a(1) + a(2)\beta$$

$$= a(0)(\beta + \beta^2) + a(1) + a(2)\beta$$

$$= a(1) + a(0) + a(2)\ \beta + a(0)\beta^2$$

$$P_1(\beta^{-1}\gamma) = a(1) = P_2(\gamma)$$

Result: $f(x) \in GF(2^3)[x]$ we have

$$P_2\left(f(x)\right) = P_1\left(\beta^{-1}f(x)\right)$$
$$P_3\left(f(x)\right) = P_1\left(\beta f(x)\right)$$

Proof: Reference Gold Notes (Page 80)

$$P_1\left(\beta f(x)\right)$$

$$P_1\left(\beta \Sigma\ f(i)x^i\right)$$

$$P_1\left(\Sigma\left(\beta f(i)\right)x^i\right)$$

$$\Sigma P_1\left(\beta f(i)\right)x^i \qquad \text{definition of } P_1$$

$$\Sigma P_3\left(f(i)\right)x^i \qquad \text{previous result}$$

$$P_3\left(\Sigma f(i)x^i\right)$$

$$P_3\left(f(x)\right)$$

[1] Study of Multi-State PN Sequences and Their Application to Communication Systems. Contract N00014-75-C-1040 - 23 July 1976.

Result: Let $a = \frac{g(x)}{f(x)}$ be a rationalized representation of a multi-state sequence where $g(x) \varepsilon GF(2^k)[x]$ and $f(x) \varepsilon GF(2)[x]$. The representation of $a = \frac{g(x)}{f(x)}$ is the interleaving of k binary sequences is given by:

$$a = \left[\frac{P_1\big(g(x)\big)}{f(x)}, \frac{P_2\big(g(x)\big)}{f(x)}, \ . \ . \ . \ \frac{P_k\big(g(x)\big)}{f(x)} \right]$$

Proof: Reference Gold Report (Page 83)

$$a = \frac{g}{f}$$

$$a \cdot f = g$$

$$P_i(a \cdot f) = P_i(g) \qquad f \varepsilon GF(2)$$

$$f \cdot P_i(a) = P_i(g) \qquad \text{see result in Gold Notes (Page 81)}$$

$$P_i(a) = \frac{P_i(g)}{f}$$

Result: $P_i\left[\beta^k \cdot \frac{g(x)}{f(x)}\right] = P_i\left[\frac{\beta^k g(x)}{f(x)}\right]$

Proof:

$$a = \frac{g(x)}{f(x)}$$

$$\beta^k \cdot a = \left(\beta^k\right)\left(\frac{g(x)}{f\ j}\right)$$

$$(\beta^k)(a)f(x) = (\beta^k)\ g(x)$$

$$P_i\left[(\beta^k)(a)f(x)\right] = P_i\left((\beta^k)\ g(x)\right)$$

$$f(x)P_i\left((\beta^k)\ (a)\right) = P_i\left((\beta^k)\ g(x)\right)$$

$$P_i\left[\left(\beta^k\right)\left(\frac{g(x)}{f(x)}\right)\right] = \frac{P_i\left((\beta^k)\ g(x)\right)}{f(x)}.$$

APPENDIX C

AUTOCORRELATION OF MAXIMAL LINEAR SEQUENCES OF PERIOD 63 OVER GF(8)

Sequence Polynomial $\alpha^5 x^2 + \alpha^2 x + 1$, Root v = 23

	------- REAL -------		----- IMAGINARY ----	
I	INT.	(SQRT 2)/2	INT.	(SQRT 2)/2
0	63	0	0	0
1	-1	0	0	0
2	-1	0	0	0
3	-1	0	0	0
4	-1	0	0	0
5	-1	0	0	0
6	-1	0	0	0
7	-1	0	0	0
8	-1	0	0	0
9	7	-16	-40	-16
10	-1	0	0	0
11	-1	0	0	0
12	-1	0	0	0
13	-1	0	0	0
14	-1	0	0	0
15	-1	0	0	0
16	-1	0	0	0
17	-1	0	0	0
18	-17	-32	0	32
19	-1	0	0	0
20	-1	0	0	0
21	-1	0	0	0
22	-1	0	0	0
23	-1	0	0	0
24	-1	0	0	0
25	-1	0	0	0
26	-1	0	0	0
27	7	48	8	48
28	-1	0	0	0
29	-1	0	0	0
30	-1	0	0	0
31	-1	0	0	0
32	-1	0	0	0
33	-1	0	0	0
34	-1	0	0	0
35	-1	0	0	0
36	7	48	-8	-48
37	-1	0	0	0
38	-1	0	0	0
39	-1	0	0	0
40	-1	0	0	0
41	-1	0	0	0
42	-1	0	0	0
43	-1	0	0	0
44	-1	0	0	0
45	-17	-32	0	-32
46	-1	0	0	0
47	-1	0	0	0
48	-1	0	0	0
49	-1	0	0	0
50	-1	0	0	0
51	-1	0	0	0
52	-1	0	0	0
53	-1	0	0	0
54	7	-16	40	16
55	-1	0	0	0
56	-1	0	0	0
57	-1	0	0	0
58	-1	0	0	0
59	-1	0	0	0
60	-1	0	0	0
61	-1	0	0	0
62	-1	0	0	0

End of Execution

Sequence Polynomial $\alpha^6 x^2 + \alpha x + 1$, Root α^{23}

I	REAL INT.	REAL (SQRT 2)/2	IMAGINARY INT.	IMAGINARY (SQRT 2)/2
0	63	0	0	0
1	-1	0	0	0
2	-1	0	0	0
3	-1	0	0	0
4	-1	0	0	0
5	-1	0	0	0
6	-1	0	0	0
7	-1	0	0	0
8	-1	0	0	0
9	7	48	-8	-48
10	-1	0	0	0
11	-1	0	0	0
12	-1	0	0	0
13	-1	0	0	0
14	-1	0	0	0
15	-1	0	0	0
16	-1	0	0	0
17	-1	0	0	0
18	7	-16	-40	-16
19	-1	0	0	0
20	-1	0	0	0
21	-1	0	0	0
22	-1	0	0	0
23	-1	0	0	0
24	-1	0	0	0
25	-1	0	0	0
26	-1	0	0	0
27	-17	-32	0	-32
28	-1	0	0	0
29	-1	0	0	0
30	-1	0	0	0
31	-1	0	0	0
32	-1	0	0	0
33	-1	0	0	0
34	-1	0	0	0
35	-1	0	0	0
36	-17	-32	0	32
37	-1	0	0	0
38	-1	0	0	0
39	-1	0	0	0
40	-1	0	0	0
41	-1	0	0	0
42	-1	0	0	0
43	-1	0	0	0
44	-1	0	0	0
45	7	-16	40	16
46	-1	0	0	0
47	-1	0	0	0
48	-1	0	0	0
49	-1	0	0	0
50	-1	0	0	0
51	-1	0	0	0
52	-1	0	0	0
53	-1	0	0	0
54	7	48	8	48
55	-1	0	0	0
56	-1	0	0	0
57	-1	0	0	0
58	-1	0	0	0
59	-1	0	0	0
60	-1	0	0	0
61	-1	0	0	0
62	-1	0	0	0

End of Execution

Sequence Polynomial $\alpha^4 x^2 + \alpha^5 x + 1$, Root α^{31}

I	REAL INT.	REAL (SQRT 2)/2	IMAGINARY INT.	IMAGINARY (SQRT 2)/2
0	63	0	0	0
1	-1	0	0	0
2	-1	0	0	0
3	-1	0	0	0
4	-1	0	0	0
5	-1	0	0	0
6	-1	0	0	0
7	-1	0	0	0
8	-1	0	0	0
9	-17	-32	0	-32
10	-1	0	0	0
11	-1	0	0	0
12	-1	0	0	0
13	-1	0	0	0
14	-1	0	0	0
15	-1	0	0	0
16	-1	0	0	0
17	-1	0	0	0
18	7	48	8	48
19	-1	0	0	0
20	-1	0	0	0
21	-1	0	0	0
22	-1	0	0	0
23	-1	0	0	0
24	-1	0	0	0
25	-1	0	0	0
26	-1	0	0	0
27	7	-16	-40	-16
28	-1	0	0	0
29	-1	0	0	0
30	-1	0	0	0
31	-1	0	0	0
32	-1	0	0	0
33	-1	0	0	0
34	-1	0	0	0
35	-1	0	0	0
36	7	-16	40	16
37	-1	0	0	0
38	-1	0	0	0
39	-1	0	0	0
40	-1	0	0	0
41	-1	0	0	0
42	-1	0	0	0
43	-1	0	0	0
44	-1	0	0	0
45	7	48	-8	-48
46	-1	0	0	0
47	-1	0	0	0
48	-1	0	0	0
49	-1	0	0	0
50	-1	0	0	0
51	-1	0	0	0
52	-1	0	0	0
53	-1	0	0	0
54	-17	-32	0	32
55	-1	0	0	0
56	-1	0	0	0
57	-1	0	0	0
58	-1	0	0	0
59	-1	0	0	0
60	-1	0	0	0
61	-1	0	0	0
62	-1	0	0	0

End of Execution

Sequence Polynomial $\alpha^6 x^2 + \alpha^6 x + 1$, Root α^{22}

	------- REAL -------		------ IMAGINARY ----	
I	INT.	(SQRT 2)/2	INT.	(SQRT 2)/2
0	63	0	0	0
1	-1	0	0	0
2	-1	0	0	0
3	-1	0	0	0
4	-1	0	0	0
5	-1	0	0	0
6	-1	0	0	0
7	-1	0	0	0
8	-1	0	0	0
9	7	48	-8	-48
10	-1	0	0	0
11	-1	0	0	0
12	-1	0	0	0
13	-1	0	0	0
14	-1	0	0	0
15	-1	0	0	0
16	-1	0	0	0
17	-1	0	0	0
18	7	-16	-40	-16
19	-1	0	0	0
20	-1	0	0	0
21	-1	0	0	0
22	-1	0	0	0
23	-1	0	0	0
24	-1	0	0	0
25	-1	0	0	0
26	-1	0	0	0
27	-17	-32	0	-32
28	-1	0	0	0
29	-1	0	0	0
30	-1	0	0	0
31	-1	0	0	0
32	-1	0	0	0
33	-1	0	0	0
34	-1	0	0	0
35	-1	0	0	0
36	-17	-32	0	32
37	-1	0	0	0
38	-1	0	0	0
39	-1	0	0	0
40	-1	0	0	0
41	-1	0	0	0
42	-1	0	0	0
43	-1	0	0	0
44	-1	0	0	0
45	7	-16	40	16
46	-1	0	0	0
47	-1	0	0	0
48	-1	0	0	0
49	-1	0	0	0
50	-1	0	0	0
51	-1	0	0	0
52	-1	0	0	0
53	-1	0	0	0
54	7	48	8	48
55	-1	0	0	0
56	-1	0	0	0
57	-1	0	0	0
58	-1	0	0	0
59	-1	0	0	0
60	-1	0	0	0
61	-1	0	0	0
62	-1	0	0	0

End of Execution

Sequence Polynomial $\alpha^4 x^2 + \alpha^4 x + 1$

I	REAL INT.	REAL (SQRT 2)/2	IMAGINARY INT.	IMAGINARY (SQRT 2)/2
0	63	0	0	0
1	9	0	-18	-18
2	-9	0	-18	18
3	-9	18	0	0
4	-9	18	0	0
5	-9	0	18	-18
6	9	0	18	18
7	63	0	0	0
8	9	0	-18	-18
9	-9	0	-18	18
10	-9	18	0	0
11	-9	18	0	0
12	-9	0	18	-18
13	9	0	18	18
14	63	0	0	0
15	9	0	-18	-18
16	-9	0	-18	18
17	-9	18	0	0
18	-9	18	0	0
19	-9	0	18	-18
20	9	0	18	18
21	63	0	0	0
22	9	0	-18	-18
23	-9	0	-18	18
24	-9	18	0	0
25	-9	18	0	0
26	-9	0	18	-18
27	9	0	18	18
28	63	0	0	0
29	9	0	-18	-18
30	-9	0	-18	18
31	-9	18	0	0
32	-9	18	0	0
33	-9	0	18	-18
34	9	0	18	18
35	63	0	0	0
36	9	0	-18	-18
37	-9	0	-18	18
38	-9	18	0	0
39	-9	18	0	0
40	-9	0	18	-18
41	9	0	18	18
42	63	0	0	0
43	9	0	-18	-18
44	-9	0	-18	18
45	-9	18	0	0
46	-9	18	0	0
47	-9	0	18	-18
48	9	0	18	18
49	63	0	0	0
50	9	0	-18	-18
51	-9	0	-18	18
52	-9	18	0	0
53	-9	18	0	0
54	-9	0	18	-18
55	9	0	18	18
56	63	0	0	0
57	9	0	-18	-18
58	-9	0	-18	18
59	-9	18	0	0
60	-9	18	0	0
61	-9	0	18	-18
62	9	0	18	18

End of Execution

REFERENCES

[1] Study of Multistate PN Sequences and Their Application to Communication Systems; Contract N00014-75-C-1040, 23 July 1976.

[2] Properties of Linear Binary Encoding Sequences; Robert Gold Associates, September 1978.